Exhibit A

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

The Pocket Vault System ("Pocket Vault") was in public use, on sale, sold, known in this country, or otherwise available to the public before the priority date of U.S. Pat. No. 8,352,730 ("the '730 Patent"). Features of Pocket Vault would have been apparent to a person of ordinary skill in the art using the public system, rendering the system § 102(a), (b), and/or (g) prior art. [1]

At least the following documents, or the documents referenced therein, describe the functionality of Pocket Vault:

- https://web.archive.org/web/20040602202951/http://chameleonnetwork.com/pocket_vault_info.htm ("Pocket Vault Overview")
- https://web.archive.org/web/20040529034458/http://www.chameleonnetwork.com/Articles/StrategicFinance/SF%20Comp%20v3.pdf ("Out of Pocket")
- https://web.archive.org/web/20040603023030/http://www.wired.com/news/business/0,1367,62545,00.html?tw=wn_tophead_7 ("Changes Stripes")
- U.S. Patent Application Publication No. 2003/0220876 ("Burger")
- PV Service Definition v0_12 ("Service Definition")
- Provisioning Overview ("Overview")
- Marzen Team Pro…11 Mar 2002 copy ("Marzen")
- pocket vault spec_tob copy.doc ("Spec Tob")
- TFarb VC CNI 101404 copy ("TFarb")

[1] Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the '730 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff's overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff's apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

- sec3.ppt ("Sec3")
- CitiCNI mtg 120601 Q&A ("CitiCNI")
- Visa Intl Tech Mtg 1204 v3 ("Visa Intl")
- Brookstone FAQ v4 ("Brookstone")

To the extent Plaintiff alleges that Pocket Vault does not disclose any particular limitation of the Asserted Claims of the '730 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the '730 Patent to modify the Pocket Vault reference and/or to combine the teachings of the Pocket Vault reference with other prior art references, including but not limited to the present prior art references found in Exhibit 730-A-K and 730-M-Z and the corresponding section(s) of charts for other prior art references for the '730 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was "obvious to try"; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional

citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 8,352,730	Exemplary Disclosure in Pocket Vault
1pre	A method for verifying a user during authentication of an integrated device, comprising the steps of:	Pocket Vault discloses a method for verifying a user during authentication of an integrated device. For example, Pocket Vault discloses verification using biometric data through a device. *See, e.g.,* "According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user." *Burger* at[0007]. "According to another aspect, a method for using an apparatus comprises steps of using the apparatus to authenticate an identity of a user of the apparatus, and after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal." *Burger* at [0010].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		for Consumers • financial, discount and affinity cards aggregated in one place, with complete security • secure backup and instant replacement of all wallet contents • current account status for debit, credit, identity and membership cards • promotions, coupons and discount offers delivered into consumers' "wallets" and available for use at point of purchase Pocket Vault Overview.
1A	persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;	Pocket Vault discloses persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered. For example, Pocket Vault discloses storing fingerprint information in persistent, tamper proof "write-once memory 212." Burger also discloses "a unique encrypted chip ID." *See, e.g.,* "After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. In one embodiment, the Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of FIG. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114, as described below." *Burger* At [0182].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

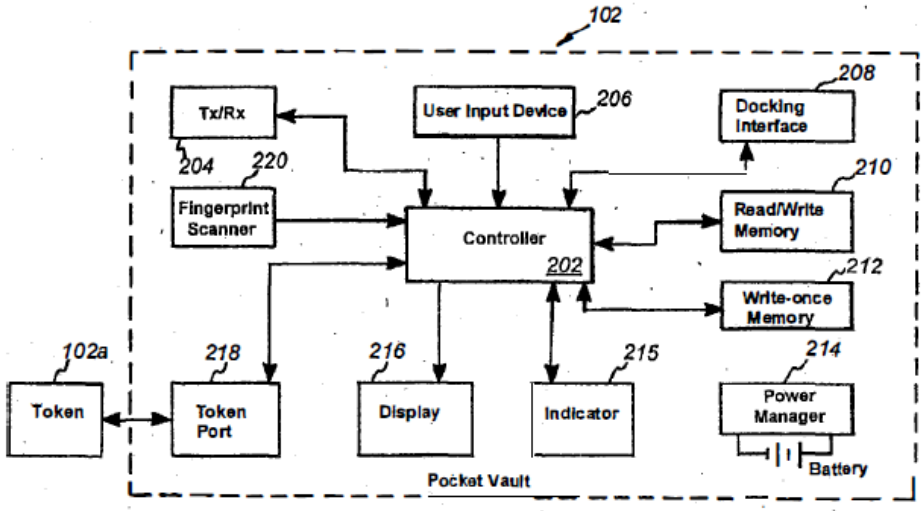


Fig. 2

"As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information."
Burger at [0114].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault 102, and the entire contents of the lost Pocket Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card." *Burger* at [0116]. for Card Issuers • Issuer becomes "portal" to customers' entire wallet contents • powerful new marketing and loyalty tools • takes customer relationships to dynamic new levels • significant reductions in fraud & operations costs for Employers • secure and centralized issuance, administration and retrieval of ID and access-control cards • supports multiple ID systems and multiple access control devices • consolidates multiple employer-issued cards onto single Pocket Vault Overview.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket. "The biometric information is stored in a secure, tamper-resistant component of the POCKET VAULT and is not stored in the Pocket Vault System." *Service Definition* at 5.4.2.1. Initialize Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer;

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." *Id.* at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

- Use a unique or random encryption method that makes each wallet different from others.
- Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet.
- Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear.
- Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code."

Id. at 10-11.

10.11.1 PV Configuration Data Dictionary

Attribute	Definition
ID	This is an internal identifier that is unique within this instantiation of the ***Pocket Vault System***.
Status	This is the current status. • `WIP`: Partially created, but not ready for use • `Active`: Fully created and ready for use. • `Inactive`: The **PV CONFIGURATION** is no longer used and can be purged from the system.
Name	This is the Name of the **PV CONFIGURATION**.
Start Date	This is the date the **PV CONFIGURATION** was created.
End Date	This is the date the **PV CONFIGURATION** is no longer in use.
Time-out Period	The amount of time, in minutes, before the **POCKET VAULT** goes to the `Locked` Status which prevents further activity without reauthentication.
▶	

Id. at 68.

"Register Pocket Vault

This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id.* at 4. "Customer use a. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. b. Financial transactions – When using the Pocket Vault for financial transactions the consumer:

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

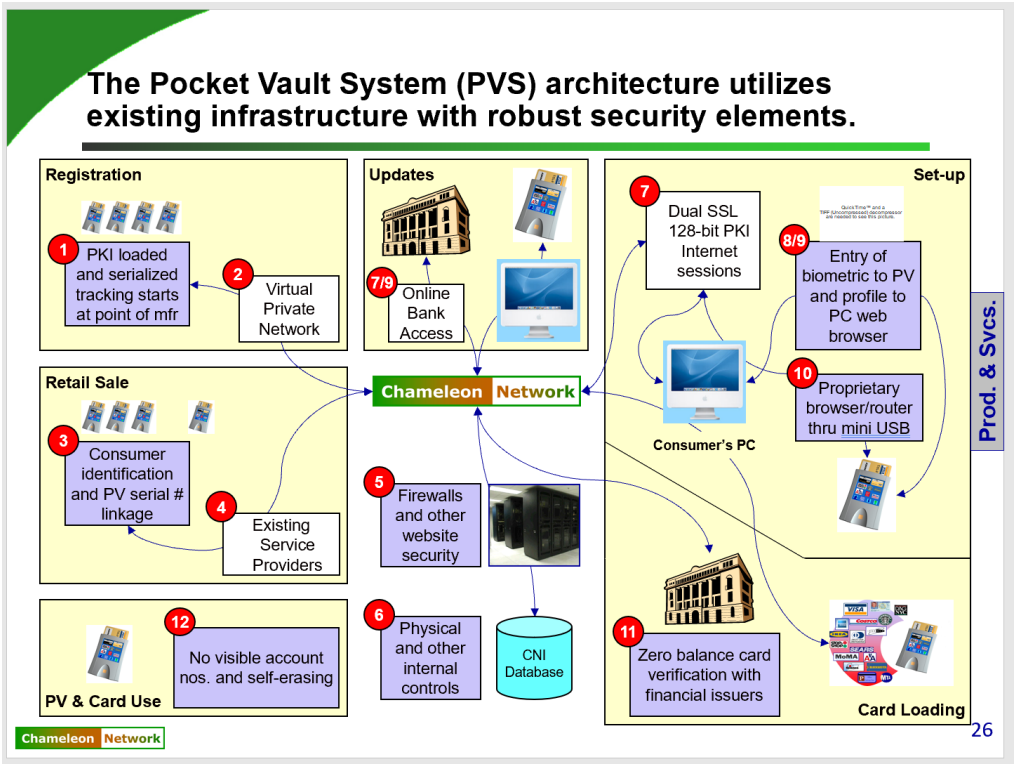
		 TFarb at 26.
1B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;	Pocket Vault discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition. *See, e.g.*, "In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in FIG. 2." *Burger* at [0107]. "As discussed below in more detail, in some embodiments of the invention, certain uses of the Pocket Vault 102, as well as each of the interface stations 104 a-c, may be permitted only by pre-authorized individuals. To this end, a suitable user authentication technique may be employed in connection with each attempted use of any of these devices. One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis. Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder's identity. In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly." *Burger* at [0112].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "The biometric information is stored in a secure, tamper-resistant component of the POCKET VAULT and is not stored in the Pocket Vault System." *Service Definition* at 5.4.2.1. Initialize Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: ○ Dock the PV set up a PV account; ○ Define information necessary to reliably identify the customer; ○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." Service Definition at 10-11.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

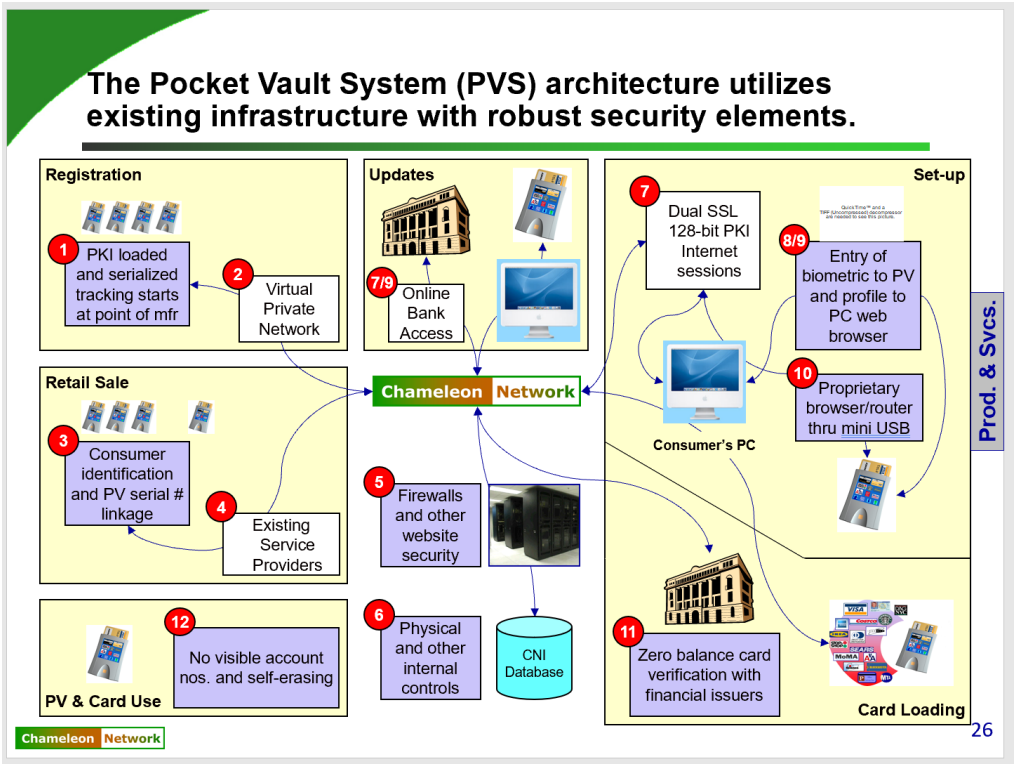
		 TFrab at 26.
1C	responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;	Pocket Vault discloses responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan. For example, Pocket Vault discloses scanning a user fingerprint when user's finger is placed on a biometric sensor. *See, e.g.*, "When, at the step 1302, it is determined that a first encrypted message including a Pocket Vault ID has been received from the Pocket Vault 102, the

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		routine 1300 proceeds to a step 1304, wherein the first encrypted message is forwarded to the interface station computer 304 (FIG. 3) After the step 1304, the routine 1300 proceeds to steps 1306 and 1308, wherein it is determined whether a fingerprint has been scanned by the fingerprint scanner 316 of the pocket vault interface unit 302 before a timeout period measured by the step 1308 has elapsed. When, at the steps 1306 and 1308, it is determined that a fingerprint has not been scanned within the timeout period of step 1308, the routine 1300 returns to the step 1346 (discussed above). When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302." *Burger* at [0345]-[0348].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

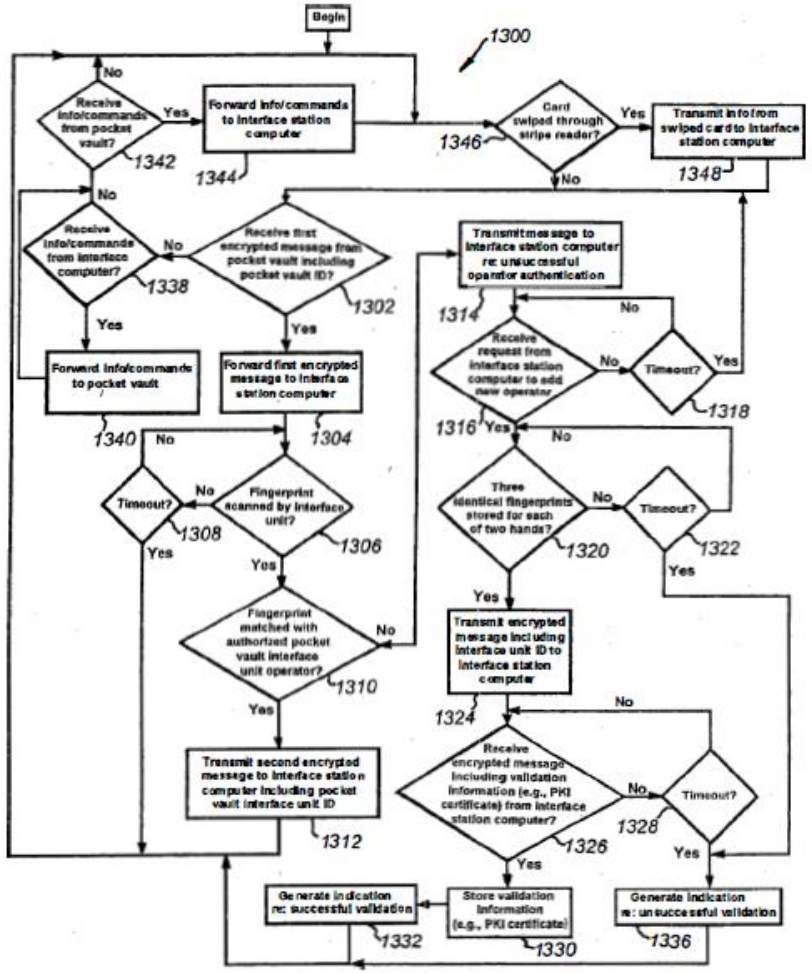


Fig. 13

"As shown, the routine 3024 begins at a step 3302, wherein it is determined whether the Pocket Vault 102 has been authenticated, e.g., whether the Pocket

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		Vault 102 has determined that a fingerprint applied to the fingerprint scanner 220 matches one of the fingerprints stored in the fingerprint memory of the Pocket Vault 102. This authentication procedure may operate as described above in connection with the step 712 (FIG. 7), or an additional or different routine may be employed (e.g., as part of the security module 2812 described above in connection with FIG. 28) to determine whether the holder has successfully authenticated his or her identity, thereby enabling the network server 114 to establish a "trust" relationship with the Pocket Vault 102." *Burger* at [0595]. By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder. 

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		Out of Pocket. First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." *Service Definition* at 5.5.1.2.1. Unlock Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: ○ Dock the PV set up a PV account; ○ Define information necessary to reliably identify the customer; ○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		• Gaining access to any fingerprint templates at any time." Spec Tob at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

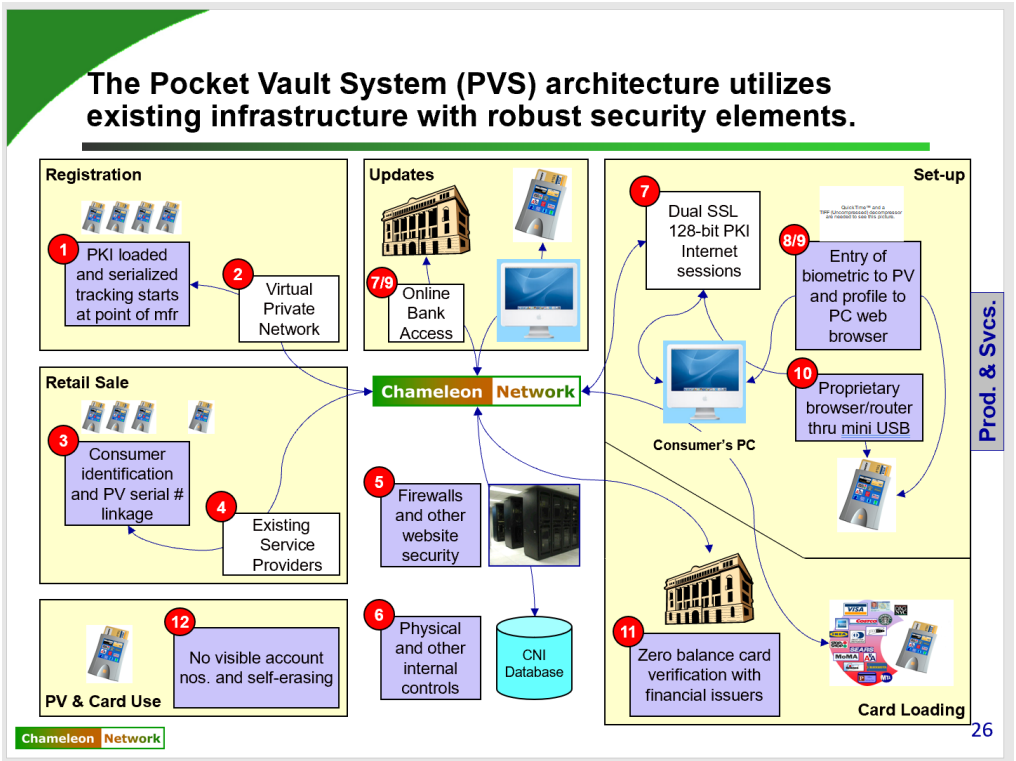
		 TFrab at 26.
1D	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;	Pocket Vault discloses comparing the scan data to the biometric data to determine whether the scan data matches the biometric data. For example, Pocket Vault discloses comparing the fingerprint image with the fingerprint template. *See, e.g.*, "When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302." *Burger* at [0348]. "When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212." *Burger* at [0184]. "When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (FIG. 7) matches one of the stored fingerprints." *Burger* at [0209]. "After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match)." *Burger* at [0336]. First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." *Service Definition* at 5.5.1.2.1. Unlock Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: ○ Dock the PV set up a PV account; ○ Define information necessary to reliably identify the customer; ○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units."

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		Märzen at 3.
1E	responsive to a determination that the scan data matches the biometric data,	Pocket Vault discloses responsive to a determination that the scan data matches the biometric data. For example, Pocket Vault discloses taking action only if acquired biometric data matches stored biometric information. *See, e.g.*, "When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302." *Burger* at [0348]. "When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212." *Burger* at [0184]. "When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (FIG. 7) matches one of the stored fingerprints." *Burger* at [0209]. "After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match)." *Burger* at [0336].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." Service Definition at 5.5.1.2.1. Unlock Pocket Vault. "This subprocess is used by the RESELLER to prevent a POCKET VAULT from ever being used again. The subprocess is used when the POCKET VAULT is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the POCKET VAULT ID and changes its status to one that prevents its use of the reuse of the specific POCKET VAULT ID." *Id.* at 5.3.2.2.4 Remove Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: ○ Dock the PV set up a PV account; ○ Define information necessary to reliably identify the customer; ○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.
1F	wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and	Pocket Vault discloses wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code. For example, Pocket Vault discloses transmitting an encrypted message including an ID of the pocket vault to the interface station computer and network server for authentication in various process. *See, e.g.,* "According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user." *Burger* at[0007]. "When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		fingerprint match, is transmitted to the interface station computer 304." *Burger* at [0349]. "According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus." *Burger* at [0019]. "When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device." *Burger* at [0186]. "When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. "When, at the step 2306, it is determined that the secure media issuer is a Pocket Vault participant, the routine 1918 proceeds to a step 2310, wherein the media issuer is queried as to the account status of the holder. After the step 2310, the routine 1918 proceeds to a step 2312, wherein it is determined whether authorization has been received from the media issuer to load the file." *Burger* at [0506].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (FIG. 4). As shown, the logged information may include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction. After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107). *Burger* at [0516]-[0518]. When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the Pocket Vault ID (if available) is linked to the ID of the entity proposing the transaction, e.g., a commercial interface station 104 c, a card reader 106, a barcode reader 107, or an RFID interrogator 107. *Burger* at [0526]. After the step 3410, the routine proceeds to a step 3412, wherein the website on the network server 114 determines whether the account for the card is valid. This determination may be made, for example, by confirming that the card is owned by the person attempting to add it to his or her Pocket Vault 102, that the card has not expired, etc. *Burger* at [0620]. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT;

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		• The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "5.4.1.2.4 Establish Wireless Pocket Vault Session A PV User or PV Manager can receive updates even when not docked to a PC. This subprocess can only be initiated after successful completion of the Unlock Pocket Vault subprocess. The PV User or PV Manager navigates to the POCKET VAULT icon to start the wireless session. • Request Update / Set session timeout • Establish secure PV to Pocket Vault System session • Initiate Update Pocket Vault process"

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

Id. at 41.

10.11.1 PV Configuration Data Dictionary

Attribute	Definition
ID	This is an internal identifier that is unique within this instantiation of the ***Pocket Vault System***.
Status	This is the current status. • `WIP`: Partially created, but not ready for use • `Active`: Fully created and ready for use. • `Inactive`: The **PV CONFIGURATION** is no longer used and can be purged from the system.
Name	This is the Name of the **PV CONFIGURATION**.
Start Date	This is the date the **PV CONFIGURATION** was created.
End Date	This is the date the **PV CONFIGURATION** is no longer in use.
Time-out Period	The amount of time, in minutes, before the **POCKET VAULT** goes to the `Locked` Status which prevents further activity without reauthentication.
▶	

Id. at 68.

"The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond."
Spec Tob at 5.

"To do this, the wallet must do at least the following:
- Store all credit card and fingerprint information in an encrypted form.
- Use a unique or random encryption method that makes each wallet different from others.
- Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		□ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id.* at 10-11. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id.* at 4. "Customer use c. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website

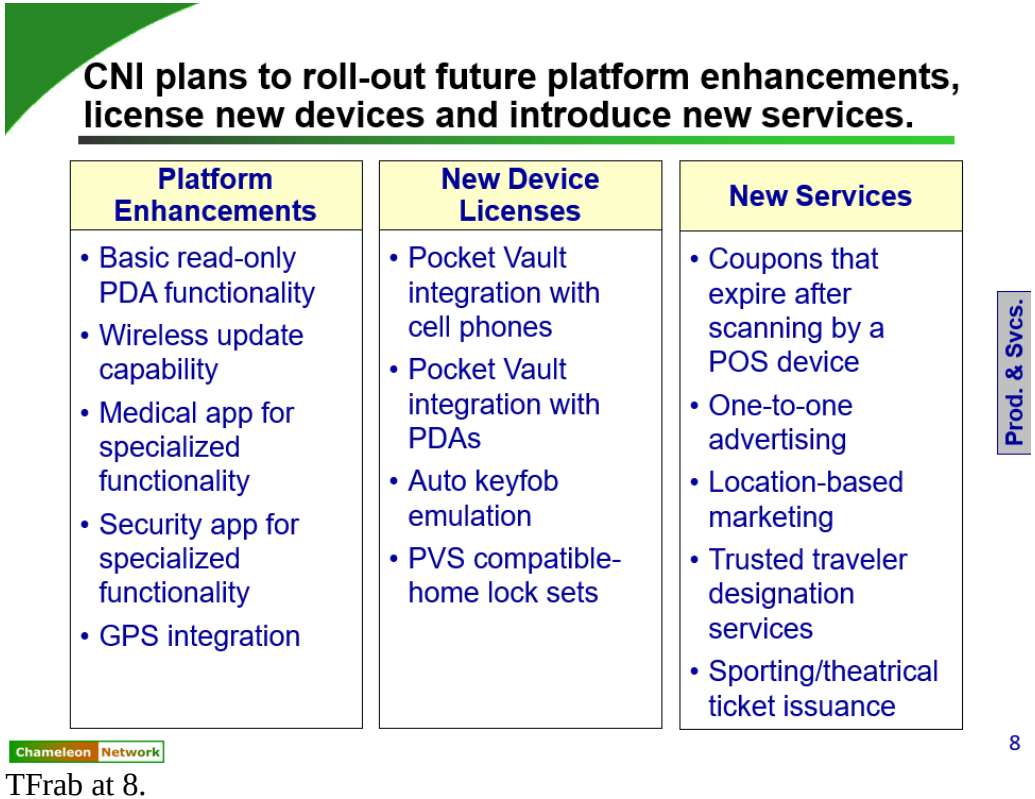
Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. d. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

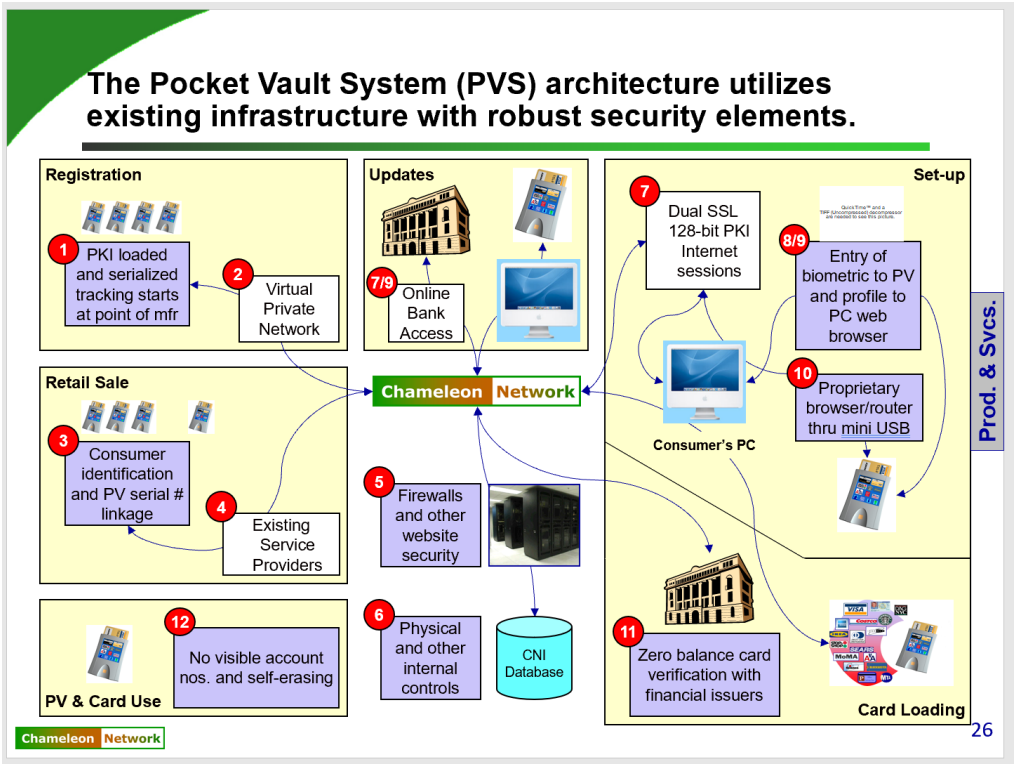
		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandiz ing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



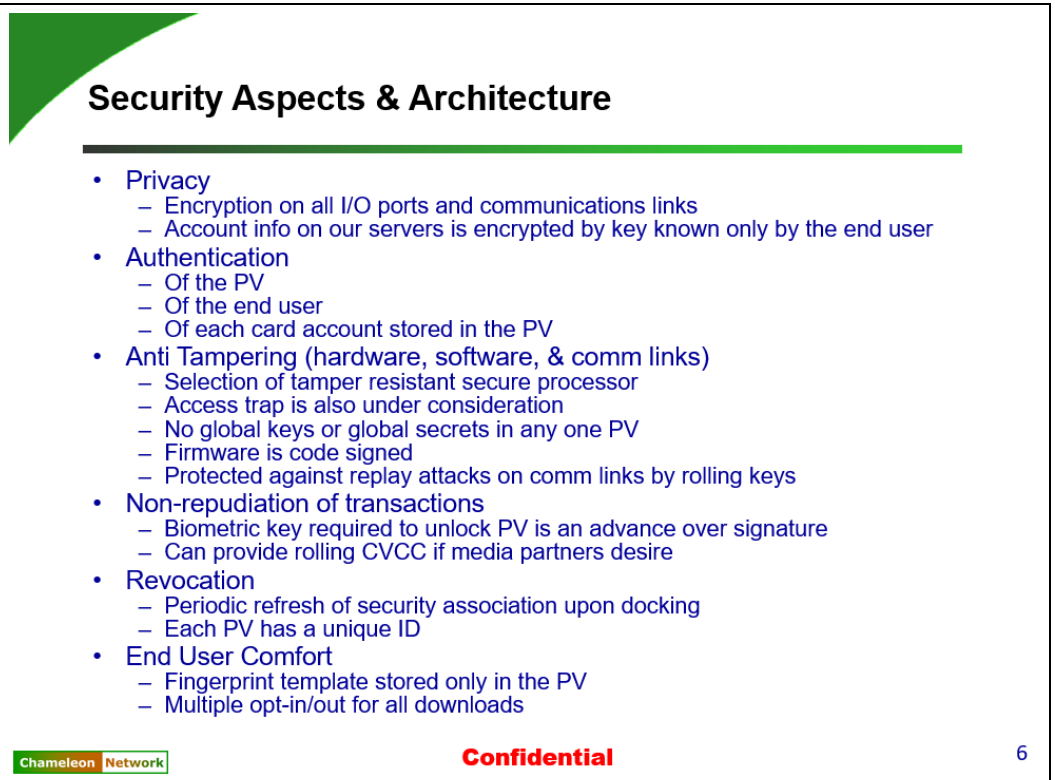
TFrab at 8.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



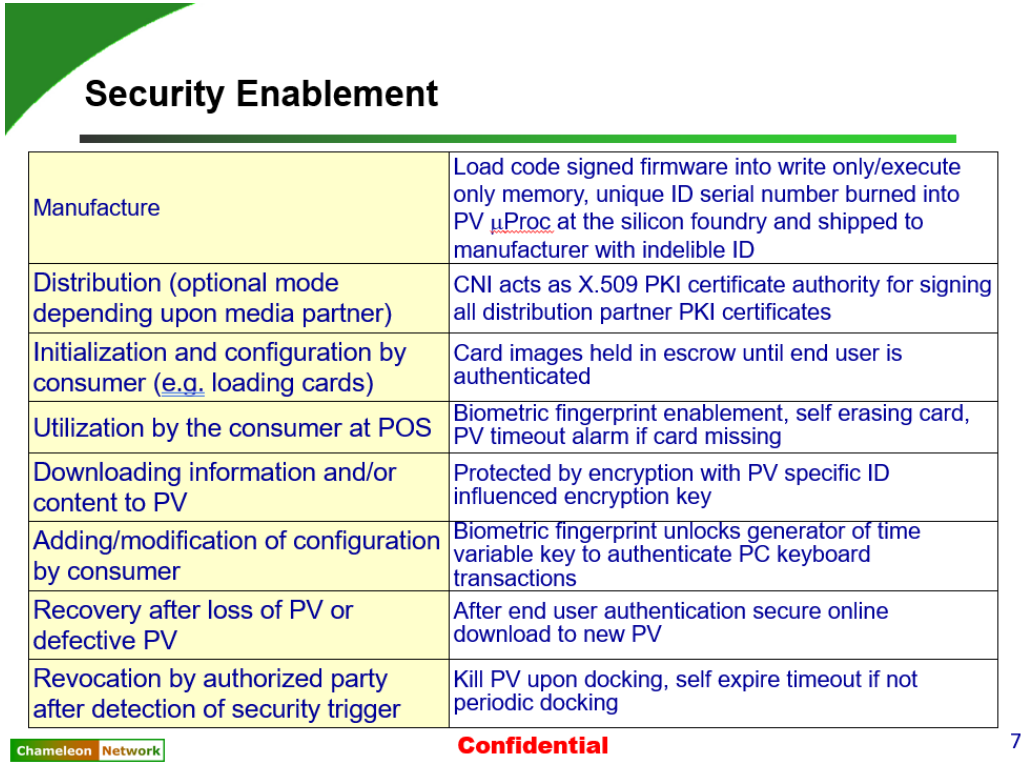
TFrab at 26.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 6.
</td>
</tr>
</table>

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 7.</td>
</tr>
<tr>
<td>1G</td>
<td>responsive to authentication of the one or more codes and the other data values by the agent,</td>
<td>Pocket Vault discloses responsive to authentication of the one or more codes and the other data values by the agent.

For example, Pocket Vault discloses making a determination whether a Pocket Vault ID is valid.

See, e.g.,

“When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is</td>
</tr>
</table>

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. When, at the step 2508, it is determined that the Pocket Vault ID is linked to the ID of the entity proposing the transaction, or that the ID of the Pocket Vault is not required, the routine 2006 proceeds to a step 2512, wherein the Pocket Vault use is authorized. *Burger* at [0528]. When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is valid, the routine 3314 proceeds to a step 3416, wherein the information for the card is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712. *Burger* at [0624]. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code."

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

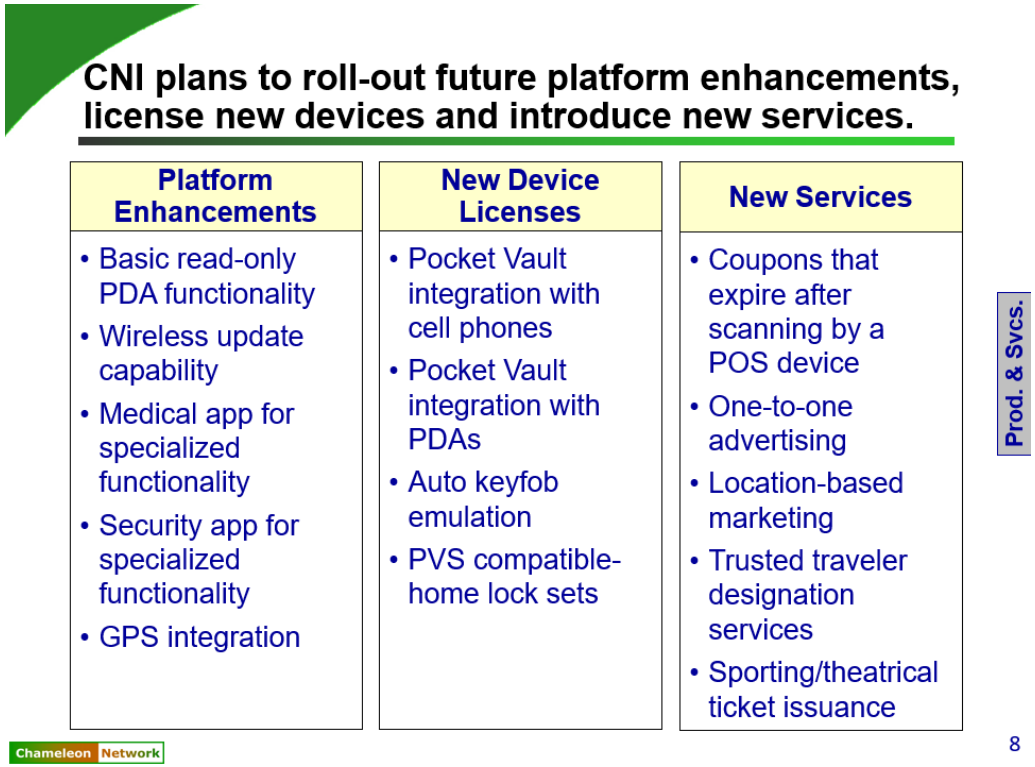
		Id. at 10-11. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault."

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id.* at 4. By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder. 

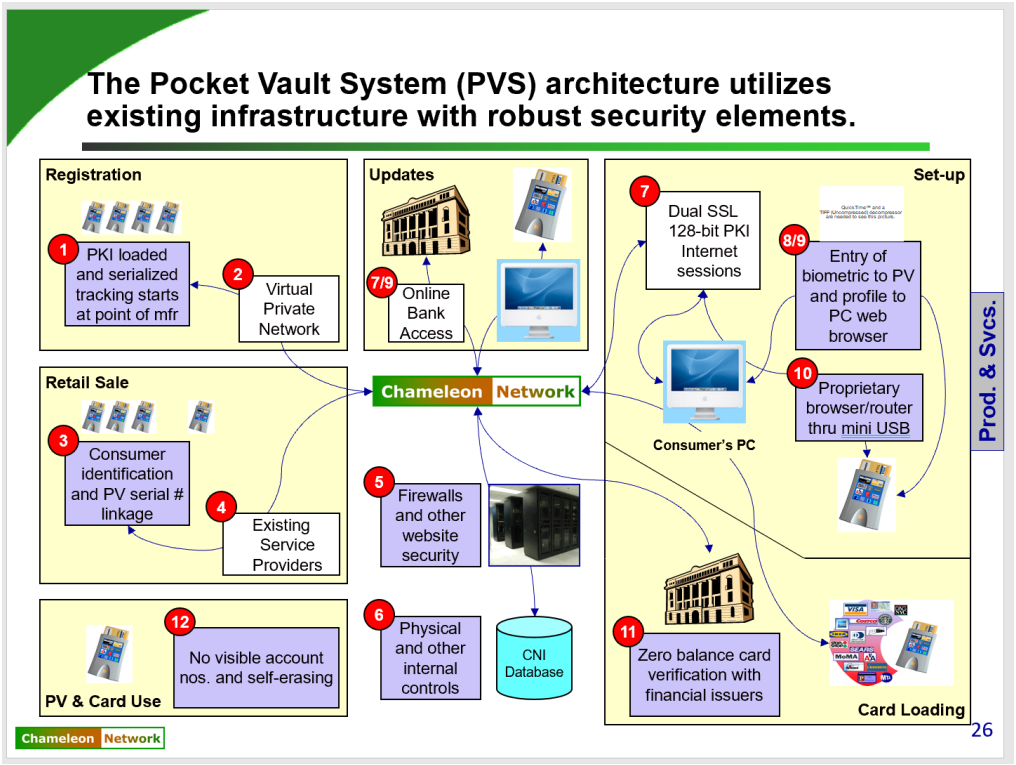
Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

Out of Pocket.



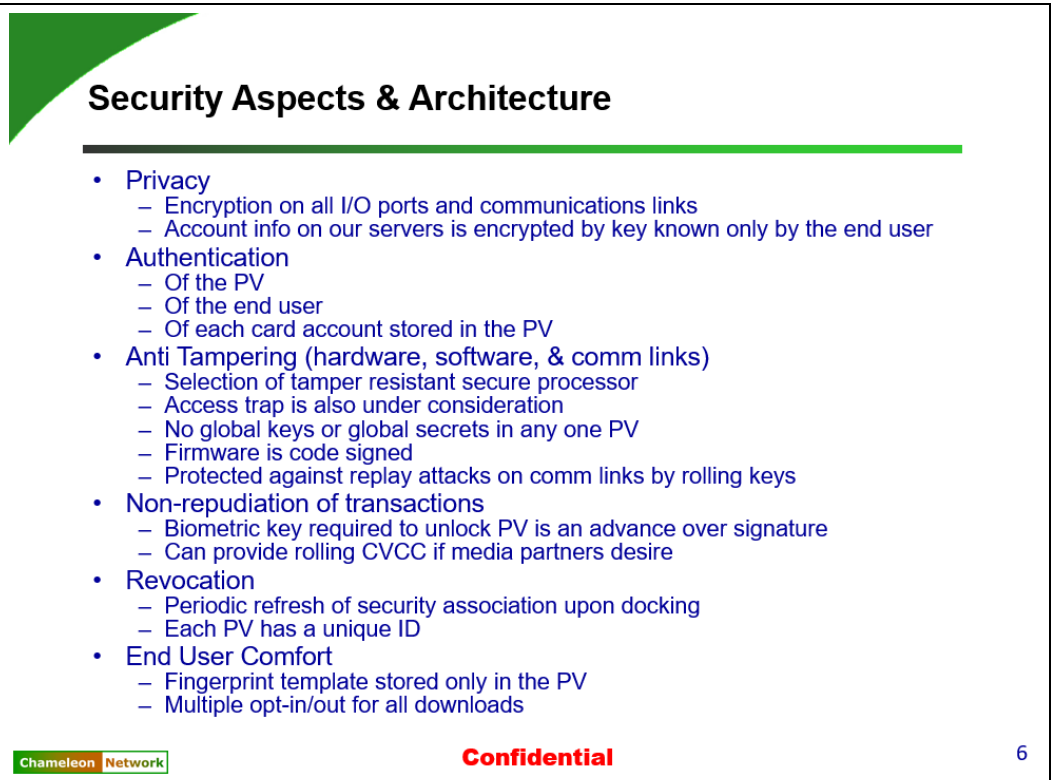
TFrab at 8.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



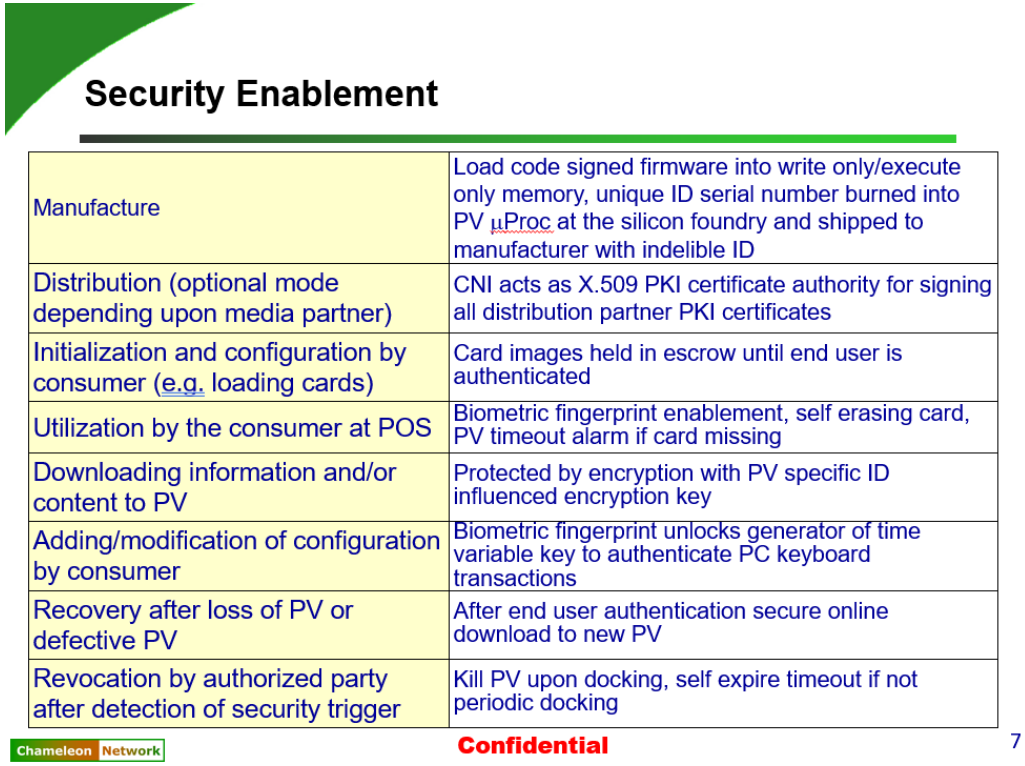
TFrab at 26.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



Sec3 at 6.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 7.</td>
</tr>
<tr>
<td>1H</td>
<td>receiving an access message from the agent allowing the user access to an application,</td>
<td>Pocket Vault discloses receiving an access message from the agent allowing the user access to an application.

For example, Pocket Vault discloses an encrypted transaction approval message, digital certificate, or internet settings used for access certain function in various process.

See, e.g.,</td>
</tr>
</table>

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID. After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732. When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed." *Burger* at [0437]-[0439] In the embodiment shown, the communication software 2710 uses internet settings 2722 when accessing the network 2724. The internet settings 2710 may include any user preferences or software settings relevant to communication functions and usability of the communication software 2710. The internet settings 2722 may comprise, for example, the network name and the identification of the interface station computer 304, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc. *Burger* at [0535]. 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107). *Burger* at [0517].

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		## Pocket Vault Overview *Pocket Vault System* replaces a consumer's conventional wallet and stores an entire wallet's contents in digital form (credit, ATM, identification, physical and network access, membership, discount cards), in a stand-alone device or integrated into PDAs and mobile phones. The Pocket Vault programs a single, "morphing" Chameleon Card to emulate the characteristics of any magnetic stripe, barcode or smart card that the user selects. The Pocket Vault and Chameleon Card are useable everywhere (brick & mortar and online), and are completely compatible with all existing point-of-sale terminals. Pocket Vault Overview. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35.

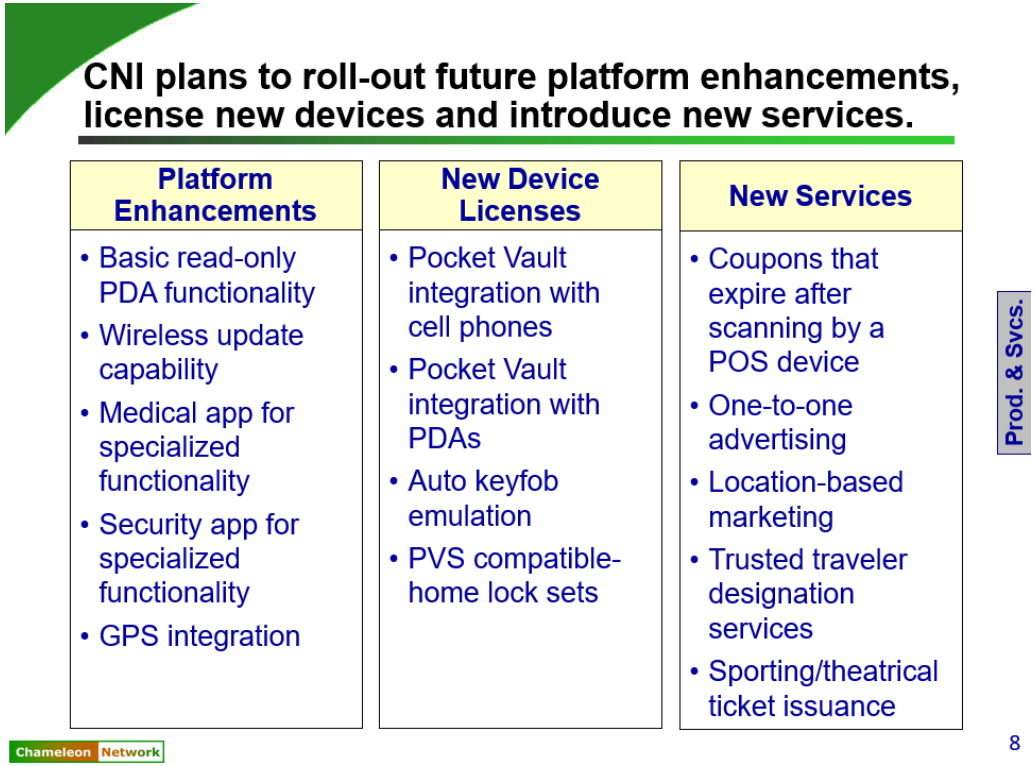
Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id.* at 10-11.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

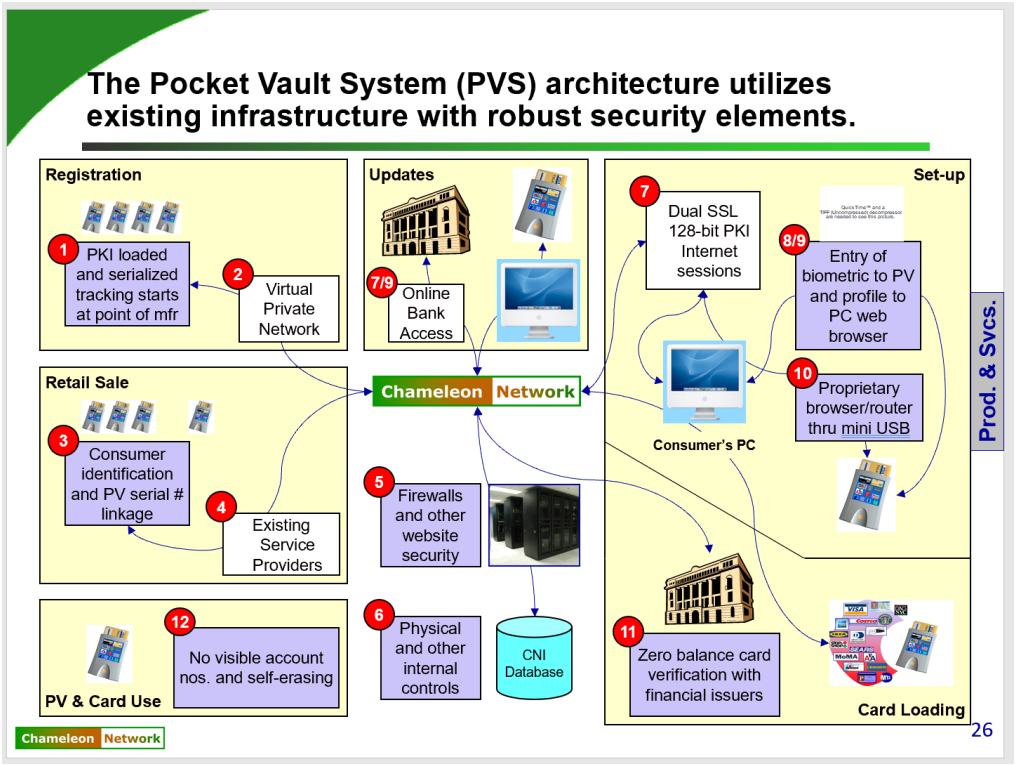
		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



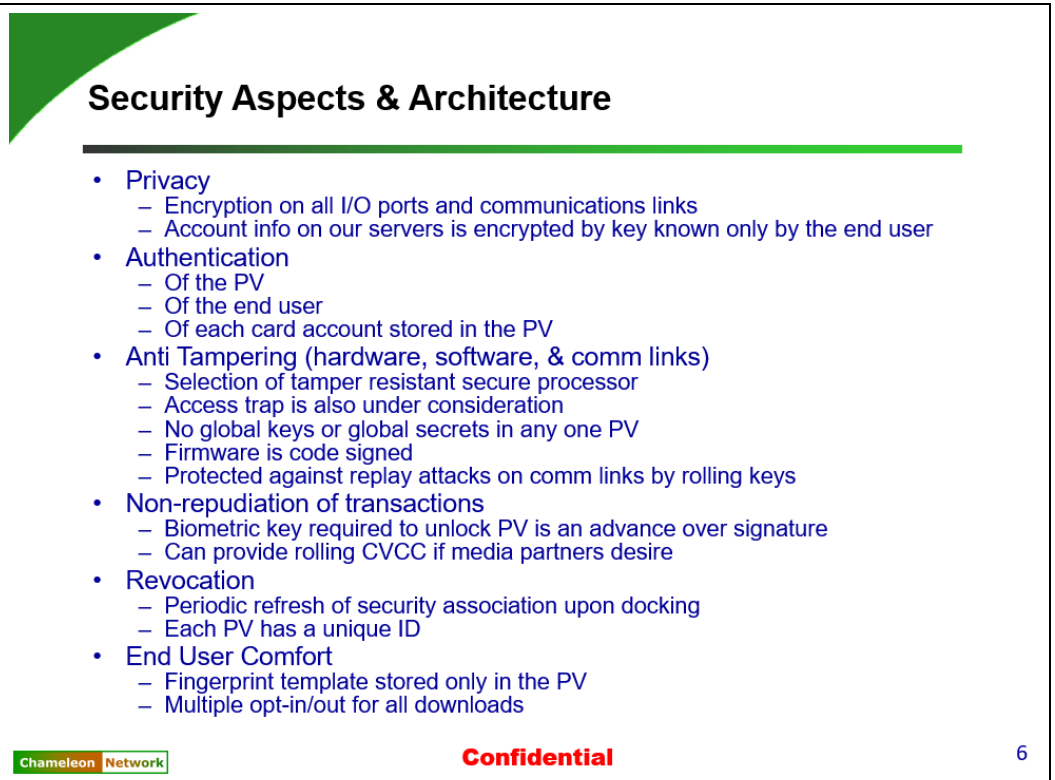
TFrab at 8.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



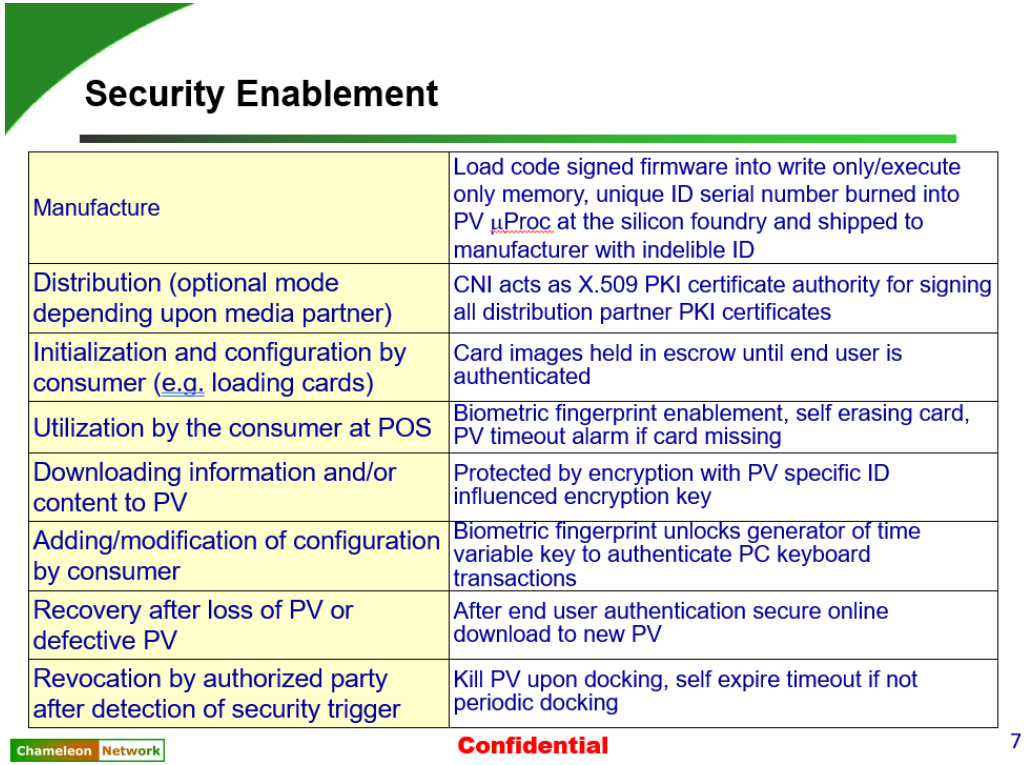
TFrab at 26.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



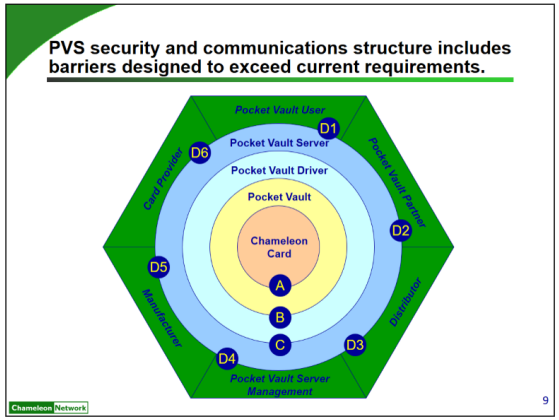
Sec3 at 6.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



Sec3 at 7.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


<table>
<tr><td><u>Barrier</u></td><td><u>Technologies</u></td></tr>
<tr><td><u>A</u></td><td>Encryption, bi-directional authentication, EMV standards</td></tr>
<tr><td>B</td><td>https/SSL, PKI, authentication, physical connection</td></tr>
<tr><td>C</td><td>https/SSL, authentication, firewall, PKI</td></tr>
<tr><td>D*</td><td>Authentication, https/SSL, firewall</td></tr>
<tr><td>D1</td><td>Requires PV session (B+C)</td></tr>
<tr><td>D2</td><td>VPN, PKI</td></tr>
<tr><td>D3</td><td>Post only commands</td></tr>
<tr><td>D4</td><td>VPN, PKI</td></tr>
<tr><td>D5</td><td>VPN, PKI</td></tr>
<tr><td>D6</td><td>VPN, PKI</td></tr>
<tr><td><u>Component</u></td><td><u>Technologies</u></td></tr>
<tr><td>CN Card</td><td>Card registration, auto-erase</td></tr>
<tr><td>PV commands</td><td>Tamper-resistant components, fingerprint, fixed set of allowable</td></tr>
<tr><td>PV Driver</td><td>Trusted USB driver/router</td></tr>
<tr><td>PVS</td><td>Isolated subnet for database, fixed set of allowable commands</td></tr>
</table>
Visa Intl at 9.
</td>
</tr>
<tr>
<td>1I</td>
<td>wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an</td>
<td>Pocket Vault discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.</td>
</tr>
</table>

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

	ATM machine, a hard drive, computer software, a web site and a file.	For example, Pocket Vault discloses accessing computer software, a website, a file, or all after verification of pocket vault, and use of the system to create hotel room key cards to access hotel rooms. *See, e.g.*, When, at the step 2302, it is determined that the to-be-loaded file does relate to a secure media issuer, the routine 1918 proceeds to a step 2306, wherein it is determined whether the secure media issuer is a Pocket Vault participant (i.e., a media issuer having access to the network server 114). *Burger* at [0498]. "After the step 3416, the routine 3314 proceeds to a step 3418, wherein a message is displayed that indicates the card has been successfully loaded onto the Pocket Vault 102 for use in future transactions." *Burger* at [0624]. "One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time-sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who intake room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104 b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room." *Burger* at [0676]. "As shown, the routine 1400 begins at a step 1402, wherein a menu is displayed on the display 324 of the interface station computer 304 that gives the operator of the interface station computer 304 several options to choose from. These options may, for example, include: (1) the option to request that a Pocket Vault 102 be validated (i.e., permitted to store a new finger print), (2) the option to request that the information currently stored on a Pocket Vault 102 be updated (e.g., information may be uploaded from the network server 114), (3) the option to request that a transaction involving a Pocket Vault 102 be authorized, and/or (4) the option to access a website on the network server 114 and take advantage of the functionality thereof." *Burger* at [0365] Pocket Vault Overview *Pocket Vault System* replaces a consumer's conventional wallet and stores an entire wallet's contents in digital form (credit, ATM, identification, physical and network access, membership, discount cards), in a stand-alone device or integrated into PDAs and mobile phones. The Pocket Vault programs a single, "morphing" Chameleon Card to emulate the characteristics of any magnetic stripe, barcode or smart card that the user selects. The Pocket Vault and Chameleon Card are useable everywhere (brick & mortar and online), and are completely compatible with all existing point-of-sale terminals. Pocket Vault Overview. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT;

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		• The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		□ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id.* at 10-11. "Customer use e. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the

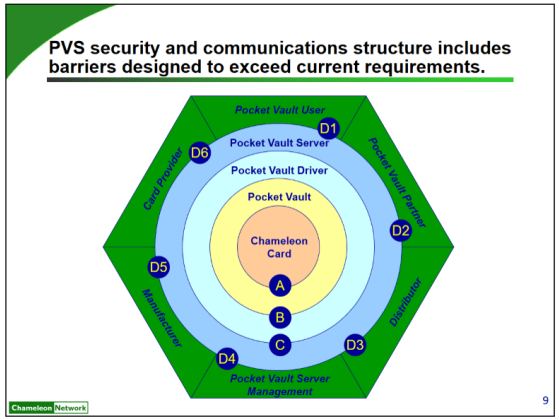
Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.)

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. f. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



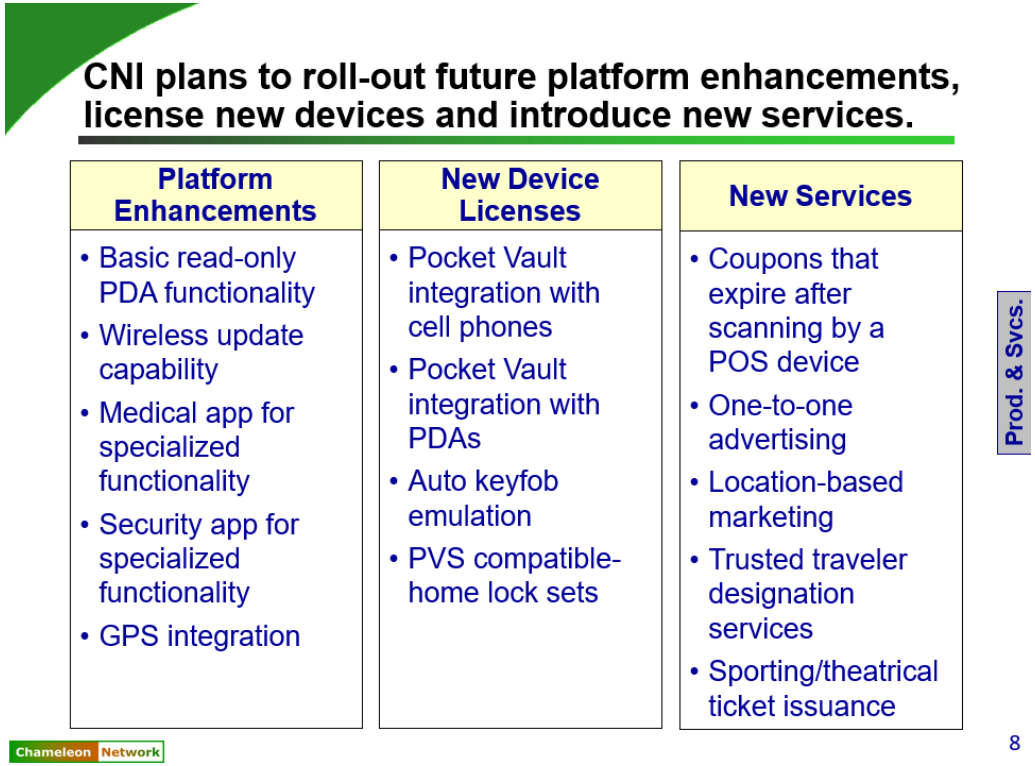
Barrier	Technologies
A	Encryption, bi-directional authentication, EMV standards
B	https/SSL, PKI, authentication, physical connection
C	https/SSL, authentication, firewall, PKI
D*	Authentication, https/SSL, firewall
D1	Requires PV session (B+C)
D2	VPN, PKI
D3	Post only commands
D4	VPN, PKI
D5	VPN, PKI
D6	VPN, PKI
Component	**Technologies**
CN Card	Card registration, auto-erase
PV commands	Tamper-resistant components, fingerprint, fixed set of allowable
PV Driver	Trusted USB driver/router
PVS	Isolated subnet for database, fixed set of allowable commands

Visa Intl at 9.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

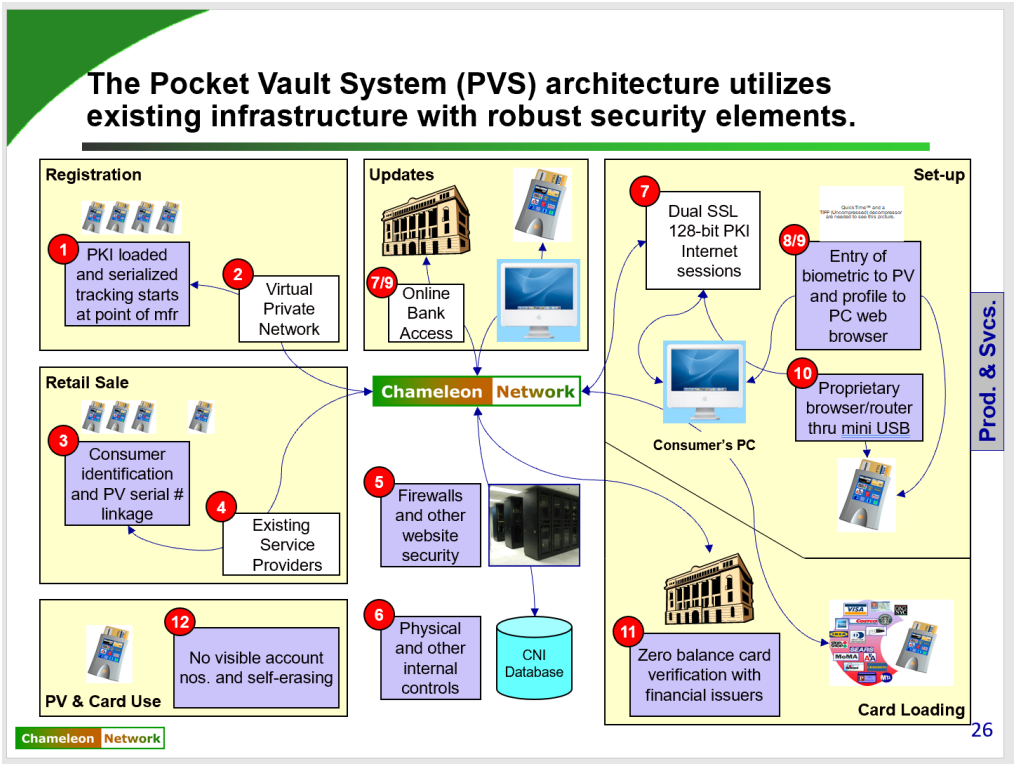
		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



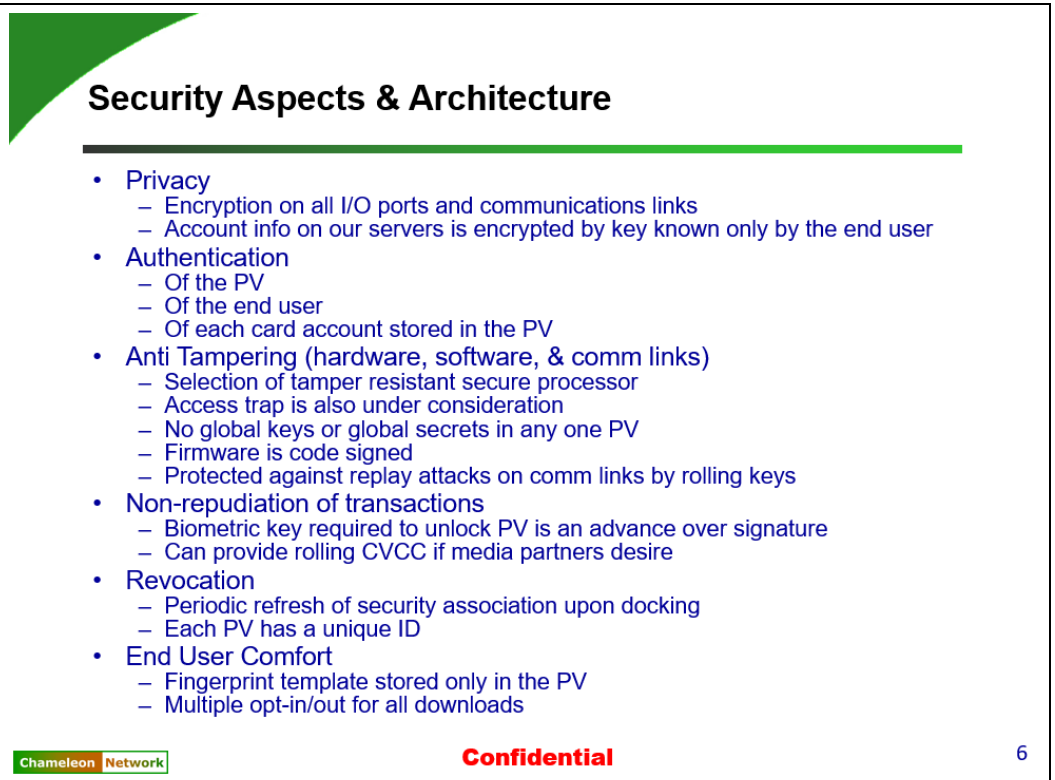
TFrab at 8.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



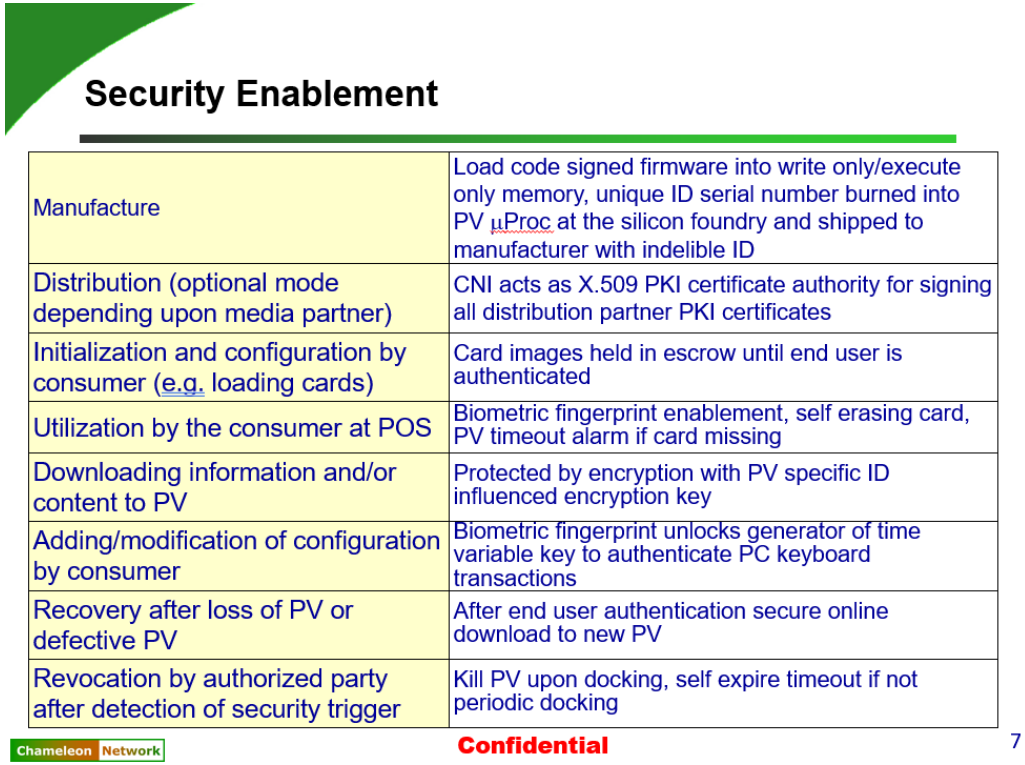
TFrab at 26.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault



Sec3 at 6.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 7.</td>
</tr>
<tr>
<td>2</td>
<td>The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.</td>
<td>Pocket Vault discloses the one or more codes and the other data values are transmitted to the agent over a network

For example, Pocket Vault discloses communications with a network server over a network.

See, e.g.,

“The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various</td>
</tr>
</table>

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		financial and non-financial media, that also may enable individuals and retailers to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns. A network system 100 configured according to one illustrative embodiment of the invention is shown in FIG. 1. As shown, the network system 100 may include a portable electronic authorization device 102 (alternatively referred to herein as a "Pocket Vault") and an associated token 102 a (alternatively referred to herein as a "Chameleon Card"). Each person desiring to use the network system 100 may possess his or her own the Pocket Vault 102 and associated token 102 a. Some individuals may choose to own multiple Pocket Vaults or Chameleon Cards. The system and software therefore may accommodate the use of multiple Pocket Vaults and multiple Chameleon Cards by one individual. Referring to FIG. 1, in addition to the Pocket Vault 102, the network system 100 may include one or more network servers 114 to which various other network components are coupled. Although multiple, load-sharing network servers 114 may be employed in a typical application, the network server(s) 114 will hereinafter, for convenience, occasionally be referred to as a single network server 114. Coupled to the network server 114 are: several different types of interface stations 104 (i.e., a validation interface station 104 a, a personal interface station 104 b, and a commercial interface station 104 c), one or more commercial card readers 106, one or more commercial bar code readers 107, one or more RFID interrogators 116, and several computers 108, 110, and 112 operated by one or more advertisers, non-financial media issuers, and financial media issuers, respectively. The structure and functionality of each of the components of the network system 100 in accordance with illustrative embodiments of the invention are described below.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		As shown in FIG. 1, the network server 114 may form the hub of the network system 100, with each of the interface stations 104, the commercial card readers 106, the commercial bar code readers 107, the RFID interrogators 116, and the computers 108, 110, and 112 being coupled thereto. As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders. Any of a number of techniques may be used to interconnect the various elements of the network system 100, and the invention is not limited to any particular networking technique. In one illustrative embodiment, for example, the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between most of the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links). *Burger* at [0095]-[0099]. "When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304." *Burger* at [0349]. "According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus." *Burger* at [0019]. "When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device." *Burger* at [0186]. "When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." Service Definition at 22. "Customer use g. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following:

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www.“pvsponsor”.com. Choose “Set up new Pocket Vault”. 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network’s 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network’s Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every

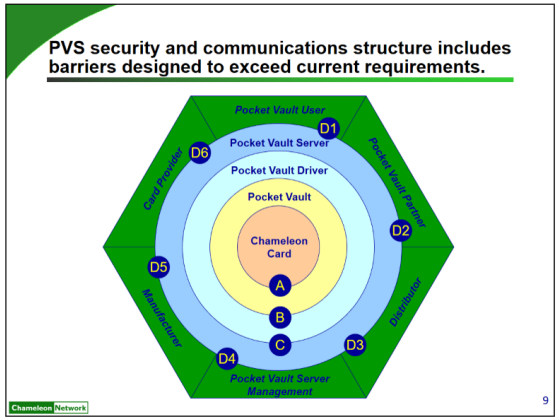
Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. h. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


<table>
<tr><th>Barrier</th><th>Technologies</th></tr>
<tr><td>A</td><td>Encryption, bi-directional authentication, EMV standards</td></tr>
<tr><td>B</td><td>https/SSL, PKI, authentication, physical connection</td></tr>
<tr><td>C</td><td>https/SSL, authentication, firewall, PKI</td></tr>
<tr><td>D*</td><td>Authentication, https/SSL, firewall</td></tr>
<tr><td>D1</td><td>Requires PV session (B+C)</td></tr>
<tr><td>D2</td><td>VPN, PKI</td></tr>
<tr><td>D3</td><td>Post only commands</td></tr>
<tr><td>D4</td><td>VPN, PKI</td></tr>
<tr><td>D5</td><td>VPN, PKI</td></tr>
<tr><td>D6</td><td>VPN, PKI</td></tr>
<tr><th>Component</th><th>Technologies</th></tr>
<tr><td>CN Card</td><td>Card registration, auto-erase</td></tr>
<tr><td>PV commands</td><td>Tamper-resistant components, fingerprint, fixed set of allowable</td></tr>
<tr><td>PV Driver</td><td>Trusted USB driver/router</td></tr>
<tr><td>PVS</td><td>Isolated subnet for database, fixed set of allowable commands</td></tr>
</table>
Visa Intl at 9.
</td>
</tr>
<tr>
<td>5</td>
<td>The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.</td>
<td>Pocket Vault discloses the biometric data and the scan data are both based on a fingerprint scan by the user.

See, e.g.,</td>
</tr>
</table>

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"It should be appreciated that, for some applications, it may be desirable to receive and store authentication information (e.g., fingerprint data) of some or all Pocket Vault holders in the network server 114. Accordingly, in some embodiments, such authentication information may be maintained by the network server 114. This authentication information may be transmitted to the network server 114, for example, when Pocket Vaults 102 are first validated." *Burger* at [0113]. By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." Service Definition at 5.5.1.2.1. Unlock Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: ○ Dock the PV set up a PV account; ○ Define information necessary to reliably identify the customer; ○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		"Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

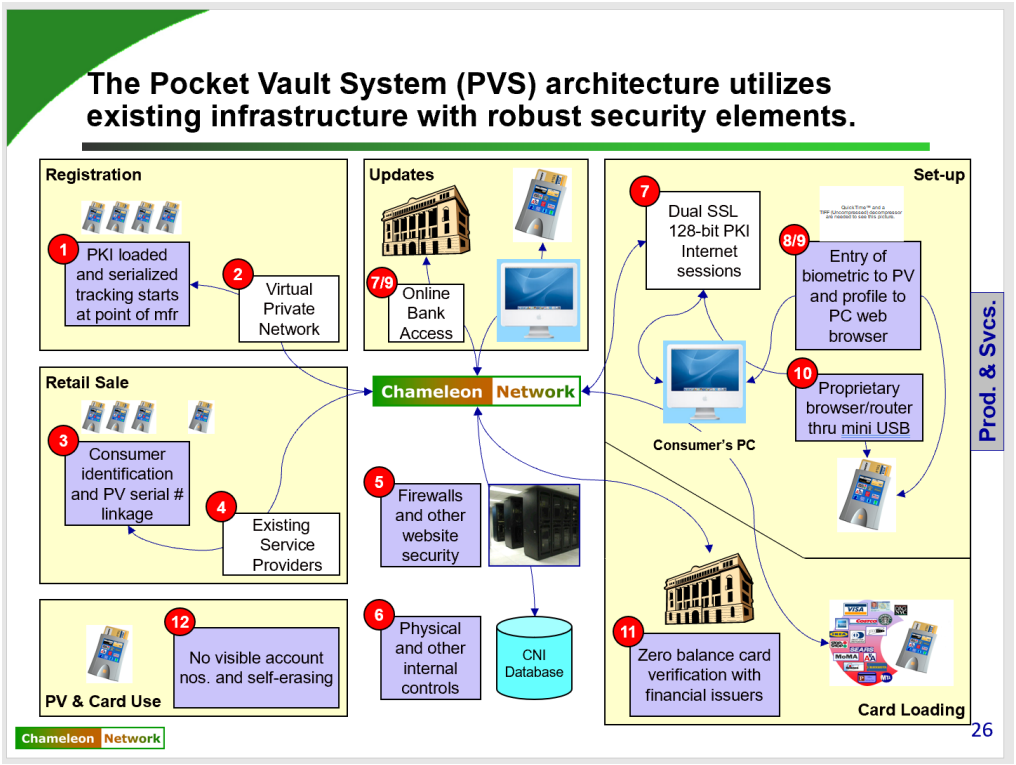
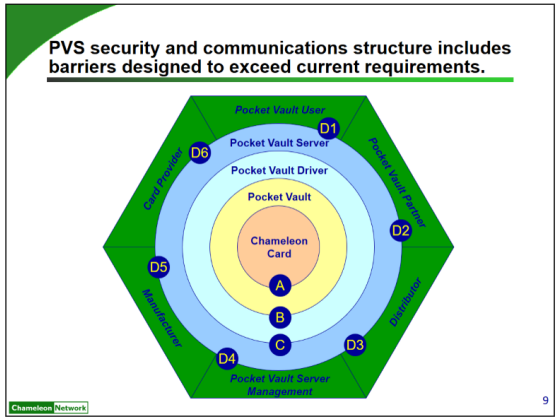
		 TFrab at 26.
6	The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.	Pocket Vault discloses establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication. For example, Pocket Vault discloses wireless transmissions between networked devices using wireless (IR or RF) links. *See, e.g.*, "Any of a number of techniques may be used to interconnect the various elements of the network system 100, and the invention is not limited to any

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

		particular networking technique. In one illustrative embodiment, for example, the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between most of the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links)." *Burger* at [0099]. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." Service Definition at 22.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


<table>
<tr><td><u>Barrier</u></td><td><u>Technologies</u></td></tr>
<tr><td><u>A</u></td><td>Encryption, bi-directional authentication, EMV standards</td></tr>
<tr><td>B</td><td>https/SSL, PKI, authentication, physical connection</td></tr>
<tr><td>C</td><td>https/SSL, authentication, firewall, PKI</td></tr>
<tr><td>D*</td><td>Authentication, https/SSL, firewall</td></tr>
<tr><td>D1</td><td>Requires PV session (B+C)</td></tr>
<tr><td>D2</td><td>VPN, PKI</td></tr>
<tr><td>D3</td><td>Post only commands</td></tr>
<tr><td>D4</td><td>VPN, PKI</td></tr>
<tr><td>D5</td><td>VPN, PKI</td></tr>
<tr><td>D6</td><td>VPN, PKI</td></tr>
<tr><td><u>Component</u></td><td><u>Technologies</u></td></tr>
<tr><td>CN Card</td><td>Card registration, auto-erase</td></tr>
<tr><td>PV commands</td><td>Tamper-resistant components, fingerprint, fixed set of allowable</td></tr>
<tr><td>PV Driver</td><td>Trusted USB driver/router</td></tr>
<tr><td>PVS</td><td>Isolated subnet for database, fixed set of allowable commands</td></tr>
</table>
Visa Intl at 9.
</td>
</tr>
<tr>
<td>8pre</td>
<td>An integrated device for verifying a user during authentication of the integrated device, comprising:</td>
<td>Pocket Vault discloses an integrated device for verifying a user during authentication of the integrated device.

See 1pre.</td>
</tr>
</table>

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

8A	a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;	Pocket Vault discloses a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered. *See* 1A.
8B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;	Pocket Vault discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition. *See* 1B.
8C	a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data,	Pocket Vault discloses a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data. *See* 1C-D.
8D	and if the scan data matches the biometric data,	Pocket Vault discloses if the scan data matches the biometric data. *See* 1E.
8E	wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the	Pocket Vault discloses wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code.

Exhibit 730-L
Invalidity Chart for U.S. Patent No. 8,352,730 In View of Pocket Vault

	one or more codes and the other data values includes the device ID code; and	*See* 1F.
8F	responsive to the agent authenticating the one or more codes and the other data values,	Pocket Vault discloses responsive to the agent authenticating the one or more codes and the other data values. *See* 1G.
8G	a radio frequency communicator, receives an access message from the agent allowing the user access to an application,	Pocket Vault discloses a radio frequency communicator, receives an access message from the agent allowing the user access to an application. *See* 1F, 1H.
8H	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.	Pocket Vault discloses wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file. *See* 1I.
9	The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.	Pocket Vault discloses the one or more codes and the other data values are transmitted to the agent over a network. *See* 2.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

The Pocket Vault System ("Pocket Vault") was in public use, on sale, sold, known in this country, or otherwise available to the public before the priority date of U.S. Pat. No. 9,289,905("the '905 Patent"). Features of Pocket Vault would have been apparent to a person of ordinary skill in the art using the public system, rendering the system § 102(a), (b), and/or (g) prior art. [1]

At least the following documents, or the documents referenced therein, describe the functionality of Pocket Vault:

- https://web.archive.org/web/20040602202951/http://chameleonnetwork.com/pocket_vault_info.htm ("Pocket Vault Overview")
- https://web.archive.org/web/20040529034458/http://www.chameleonnetwork.com/Articles/StrategicFinance/SF%20Comp%20v3.pdf ("Out of Pocket")
- https://web.archive.org/web/20040603023030/http://www.wired.com/news/business/0,1367,62545,00.html?tw=wn_tophead_7 ("Changes Stripes")
- U.S. Patent Application Publication No. 2003/0220876 ("Burger")
- PV Service Definition v0_12 ("Service Definition")
- CNIFullBizPln-v11Flaster copy ("CNIFullBizPln")
- Provisioning Overview ("Overview")
- Marzen Team Pro…11 Mar 2002 copy ("Marzen")
- pocket vault spec_tob copy.doc ("Spec Tob")

[1] Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the '905 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff's overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff's apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

- TFarb VC CNI 101404 copy ("TFarb")
- sec3.ppt ("Sec3")
- CitiCNI mtg 120601 Q&A ("CitiCNI")
- Visa Intl Tech Mtg 1204 v3 ("Visa Intl")
- Brookstone FAQ v4 ("Brookstone")

To the extent Plaintiff alleges that Pocket Vault does not disclose any particular limitation of the Asserted Claims of the '905 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the '905 Patent to modify the Pocket Vault reference and/or to combine the teachings of the Pocket Vault reference with other prior art references, including but not limited to the present prior art references found in Exhibits 905-A-K and 905-M-R and the corresponding section(s) of charts for other prior art references for the '905 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was "obvious to try"; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for

that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 9,289,905	Exemplary Disclosure in Pocket Vault
1pre	A method comprising:	Pocket Vault discloses a method. For example, Pocket Vault discloses verification using biometric data through a device. *See, e.g.,* "According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user." *Burger* at [0007]. "According to another aspect, a method for using an apparatus comprises steps of using the apparatus to authenticate an identity of a user of the apparatus, and after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal." *Burger* at [0010]. for Consumers • financial, discount and affinity cards aggregated in one place, with complete security • secure backup and instant replacement of all wallet contents • current account status for debit, credit, identity and membership cards • promotions, coupons and discount offers delivered into consumers' "wallets" and available for use at point of purchase

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		Pocket Vault Overview.
1A	persistently storing biometric data of a legitimate user and an ID code on an integrated device;	Pocket Vault discloses persistently storing biometric data of a legitimate user and an ID code on an integrated device. For example, Pocket Vault discloses storing fingerprint information in persistent, tamper proof "write-once memory 212." *Burger* [0182]. Burger also discloses "a unique encrypted chip ID." *Burger* at [0114]. *See, e.g.*, "After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. In one embodiment, the Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of FIG. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114, as described below." *Burger* at [0182].

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

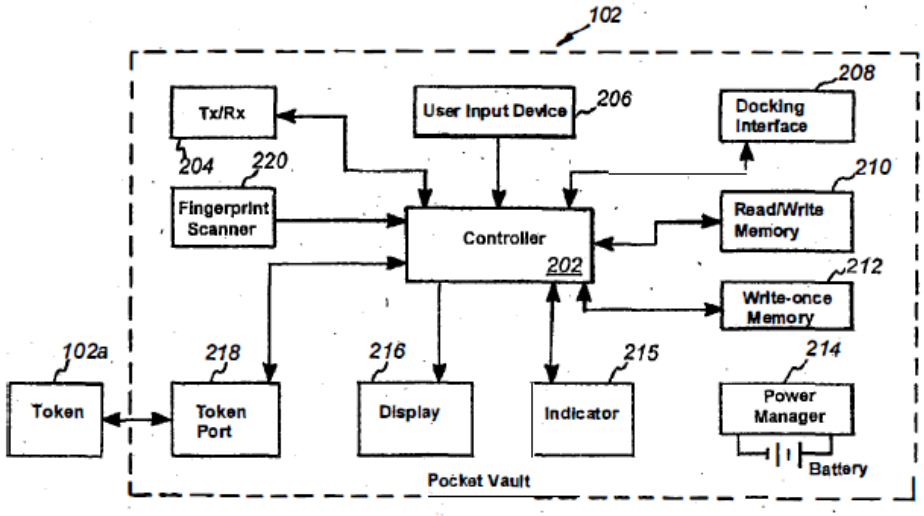


Fig. 2

"As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information." *Burger* at [0114].

"Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault 102, and the entire contents of the lost Pocket

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card." *Burger* at [0116]. for Card Issuers • Issuer becomes "portal" to customers' entire wallet contents • powerful new marketing and loyalty tools • takes customer relationships to dynamic new levels • significant reductions in fraud & operations costs for Employers • secure and centralized issuance, administration and retrieval of ID and access-control cards • supports multiple ID systems and multiple access control devices • consolidates multiple employer-issued cards onto single Pocket Vault Overview.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket. "The biometric information is stored in a secure, tamper-resistant component of the POCKET VAULT and is not stored in the Pocket Vault System." *Service Definition* at 5.4.2.1. Initialize Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer;

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." *Id*. at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id*. at 22. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

- Use a unique or random encryption method that makes each wallet different from others.
- Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet.
- Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear.
- Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code."

Id. at 10-11.

10.11.1 PV Configuration Data Dictionary

Attribute	Definition
ID	This is an internal identifier that is unique within this instantiation of the ***Pocket Vault System***.
Status	This is the current status. • `WIP`: Partially created, but not ready for use • `Active`: Fully created and ready for use. • `Inactive`: The **PV CONFIGURATION** is no longer used and can be purged from the system.
Name	This is the Name of the **PV CONFIGURATION**.
Start Date	This is the date the **PV CONFIGURATION** was created.
End Date	This is the date the **PV CONFIGURATION** is no longer in use.
Time-out Period	The amount of time, in minutes, before the **POCKET VAULT** goes to the `Locked` Status which prevents further activity without reauthentication.
▶	

Id. at 68.

"Register Pocket Vault

This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id*. at 4. "Customer use a. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. b. Financial transactions – When using the Pocket Vault for financial transactions the consumer:

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

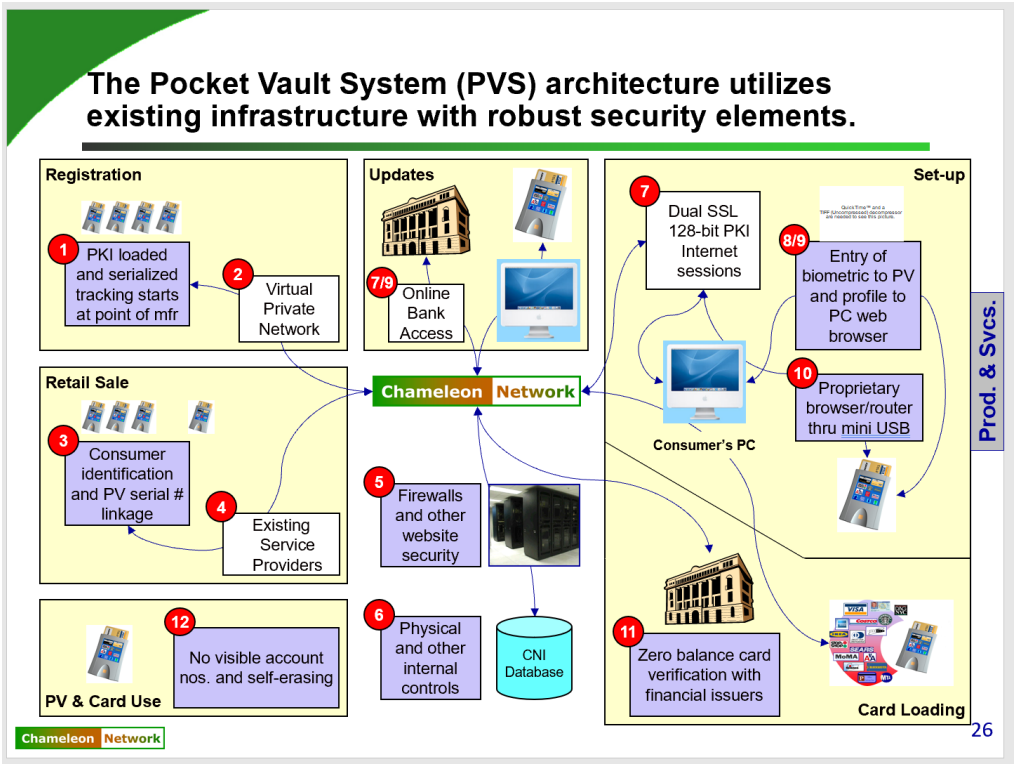
		 TFarb at 26.
1B	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;	Pocket Vault discloses responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor. For example, Pocket Vault discloses scanning a user fingerprint when user's finger is placed on a biometric sensor. *See, e.g.,*

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"When, at the step 1302, it is determined that a first encrypted message including a Pocket Vault ID has been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1304, wherein the first encrypted message is forwarded to the interface station computer 304 (FIG. 3) After the step 1304, the routine 1300 proceeds to steps 1306 and 1308, wherein it is determined whether a fingerprint has been scanned by the fingerprint scanner 316 of the pocket vault interface unit 302 before a timeout period measured by the step 1308 has elapsed. When, at the steps 1306 and 1308, it is determined that a fingerprint has not been scanned within the timeout period of step 1308, the routine 1300 returns to the step 1346 (discussed above). When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302." *Burger* at [0345]-[0348].

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

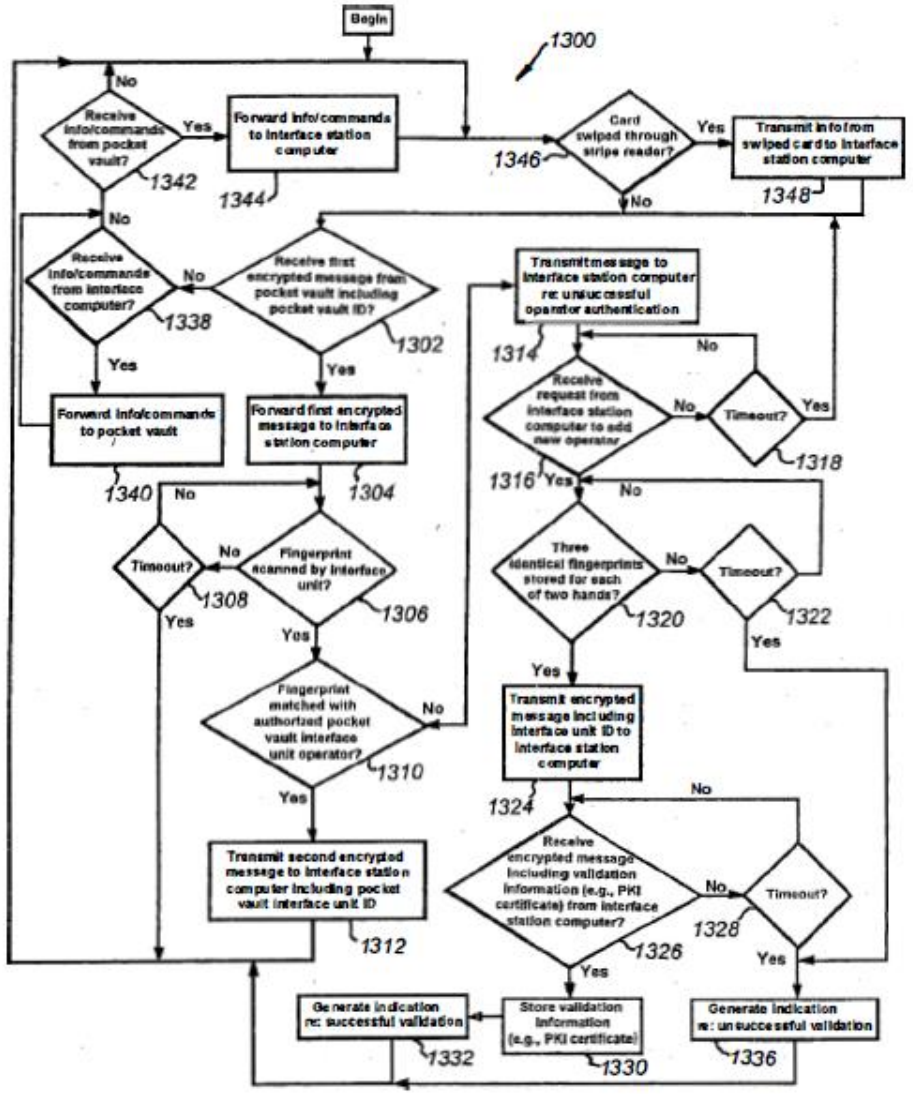


Fig. 13

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"As shown, the routine 3024 begins at a step 3302, wherein it is determined whether the Pocket Vault 102 has been authenticated, e.g., whether the Pocket Vault 102 has determined that a fingerprint applied to the fingerprint scanner 220 matches one of the fingerprints stored in the fingerprint memory of the Pocket Vault 102. This authentication procedure may operate as described above in connection with the step 712 (FIG. 7), or an additional or different routine may be employed (e.g., as part of the security module 2812 described above in connection with FIG. 28) to determine whether the holder has successfully authenticated his or her identity, thereby enabling the network server 114 to establish a "trust" relationship with the Pocket Vault 102." *Burger* at [0595].

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." *Service Definition* at 5.5.1.2.1. Unlock Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer; o Enroll at least two fingerprints to the device; o Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

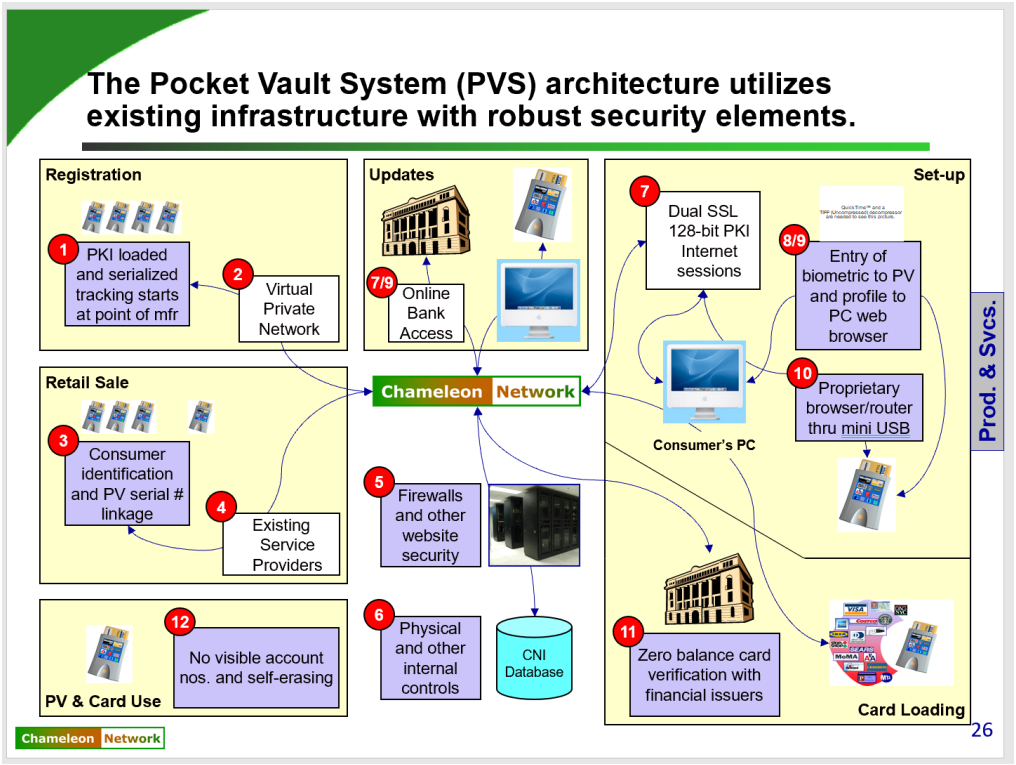
		 TFrab at 26.
1C	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;	Pocket Vault discloses comparing the scan data to the biometric data to determine whether the scan data matches the biometric data. For example, Pocket Vault discloses comparing the fingerprint image with the fingerprint template. *See, e.g.*, "When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302." *Burger* at [0348]. "When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212." *Burger* at [0184]. "When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (FIG. 7) matches one of the stored fingerprints." *Burger* at [0209]. "After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match)." *Burger* at [0336]. First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." *Service Definition* at 5.5.1.2.1. Unlock Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer; o Enroll at least two fingerprints to the device; o Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units."

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		Märzen at 3.
1D	responsive to a determination that the scan data matches the biometric data,	Pocket Vault discloses responsive to a determination that the scan data matches the biometric data, . *See* 1C.
1E	wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and	Pocket Vault discloses wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. For example, Pocket Vault discloses transmitting a second encrypted message including an ID of the pocket vault interface to the interface station computer. *See, e.g.,* "According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user." *Burger* at[0007]. "When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304." *Burger* at [0349]. "According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus." *Burger* at [0019]. "When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device." *Burger* at [0186]. "When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. "When, at the step 2306, it is determined that the secure media issuer is a Pocket Vault participant, the routine 1918 proceeds to a step 2310, wherein the media issuer is queried as to the account status of the holder. After the step 2310, the routine 1918 proceeds to a step 2312, wherein it is determined whether authorization has been received from the media issuer to load the file." *Burger* at [0506]. When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (FIG. 4). As shown, the logged information may include the identification of the entity with which the

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction. After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107). *Burger* at [0516]-[0518]. When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the Pocket Vault ID (if available) is linked to the ID of the entity proposing the transaction, e.g., a commercial interface station 104 c, a card reader 106, a barcode reader 107, or an RFID interrogator 107. *Burger* at [0526]. After the step 3410, the routine proceeds to a step 3412, wherein the website on the network server 114 determines whether the account for the card is valid. This determination may be made, for example, by confirming that the card is owned by the person attempting to add it to his or her Pocket Vault 102, that the card has not expired, etc. *Burger* at [0620]. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "5.4.1.2.4 Establish Wireless Pocket Vault Session A PV User or PV Manager can receive updates even when not docked to a PC. This subprocess can only be initiated after successful completion of the Unlock Pocket Vault subprocess. The PV User or PV Manager navigates to the POCKET VAULT icon to start the wireless session. • Request Update / Set session timeout • Establish secure PV to Pocket Vault System session • Initiate Update Pocket Vault process" *Id.* at 41.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

10.11.1 PV Configuration Data Dictionary

Attribute	Definition
ID	This is an internal identifier that is unique within this instantiation of the ***Pocket Vault System***.
Status	This is the current status. • `WIP`: Partially created, but not ready for use • `Active`: Fully created and ready for use. • `Inactive`: The **PV CONFIGURATION** is no longer used and can be purged from the system.
Name	This is the Name of the **PV CONFIGURATION**.
Start Date	This is the date the **PV CONFIGURATION** was created.
End Date	This is the date the **PV CONFIGURATION** is no longer in use.
Time-out Period	The amount of time, in minutes, before the **POCKET VAULT** goes to the `Locked` Status which prevents further activity without reauthentication.
►	

Id. at 68.

"The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond."
Spec Tob at 5.

"To do this, the wallet must do at least the following:
- Store all credit card and fingerprint information in an encrypted form.
- Use a unique or random encryption method that makes each wallet different from others.
- Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet.
- Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		□ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id*. at 10-11. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id*. at 4. "Customer use c. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.)

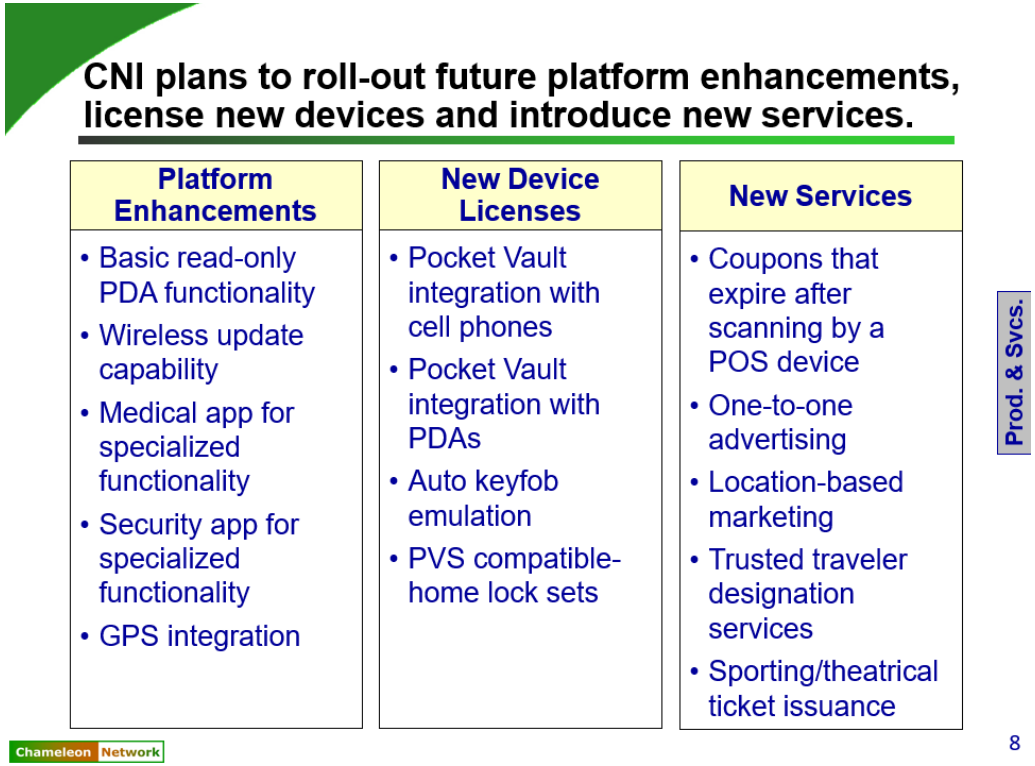
Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. d. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

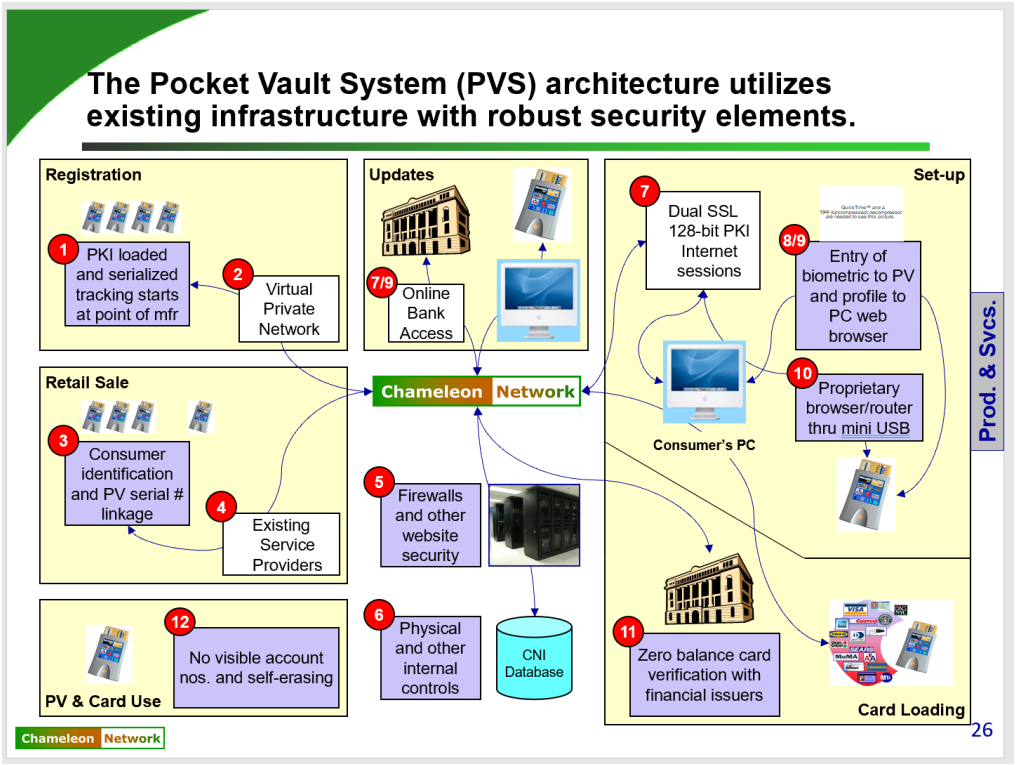
		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault



TFrab at 8.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault



TFrab at 26.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

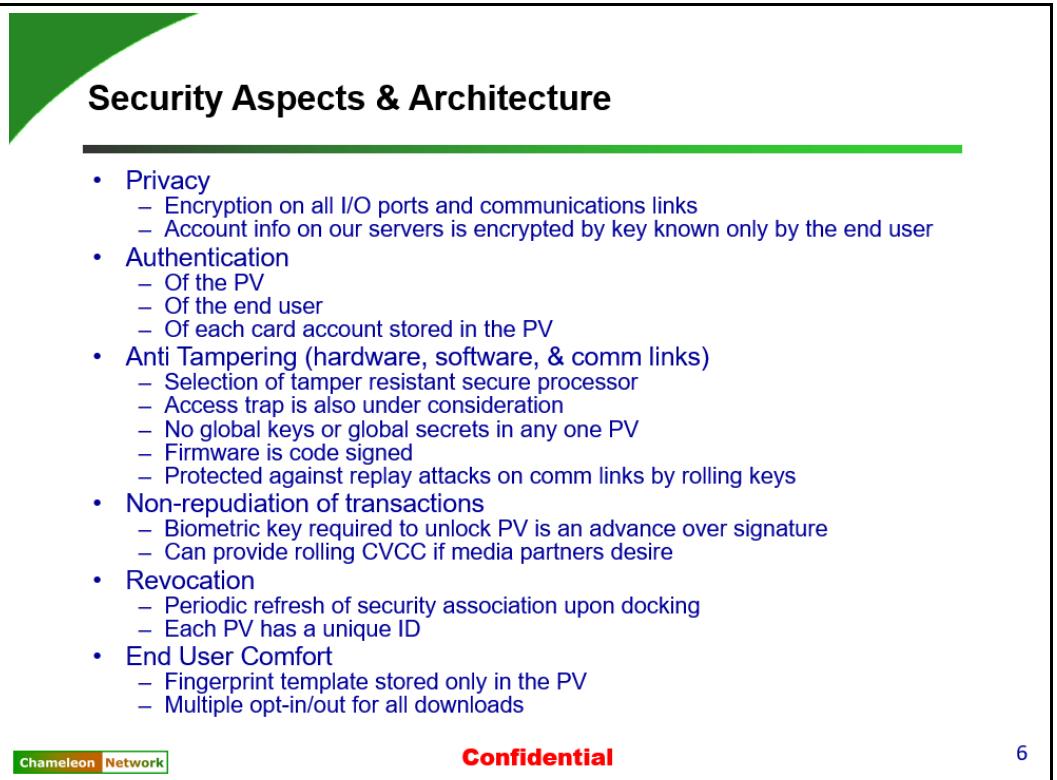
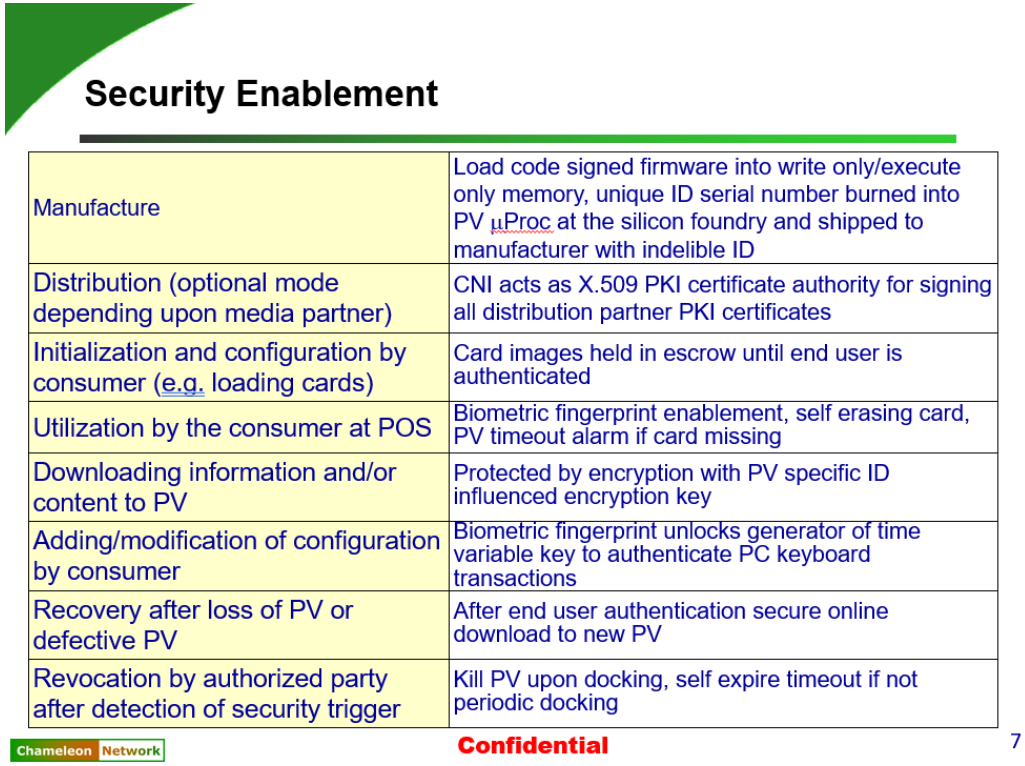
		 Sec3 at 6.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 7.</td>
</tr>
<tr>
<td>1F</td>
<td>responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code,</td>
<td>Pocket Vault discloses responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code.

For example, Pocket Vault discloses making a determination whether a Pocket Vault ID is valid.

See, e.g.,</td>
</tr>
</table>

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID. After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732. When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed." *Burger* at [0437]-[0439] In the embodiment shown, the communication software 2710 uses internet settings 2722 when accessing the network 2724. The internet settings 2710 may include any user preferences or software settings relevant to communication functions and usability of the communication software 2710. The internet settings 2722 may comprise, for example, the network name and the identification of the interface station computer 304, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc. *Burger* at [0535]. 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107). *Burger* at [0517].

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. When, at the step 2508, it is determined that the Pocket Vault ID is linked to the ID of the entity proposing the transaction, or that the ID of the Pocket Vault is not required, the routine 2006 proceeds to a step 2512, wherein the Pocket Vault use is authorized. *Burger* at [0528]. When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is valid, the routine 3314 proceeds to a step 3416, wherein the information for the card is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712. *Burger* at [0624]. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id*. at 22. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		□ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id*. at 10-11. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete

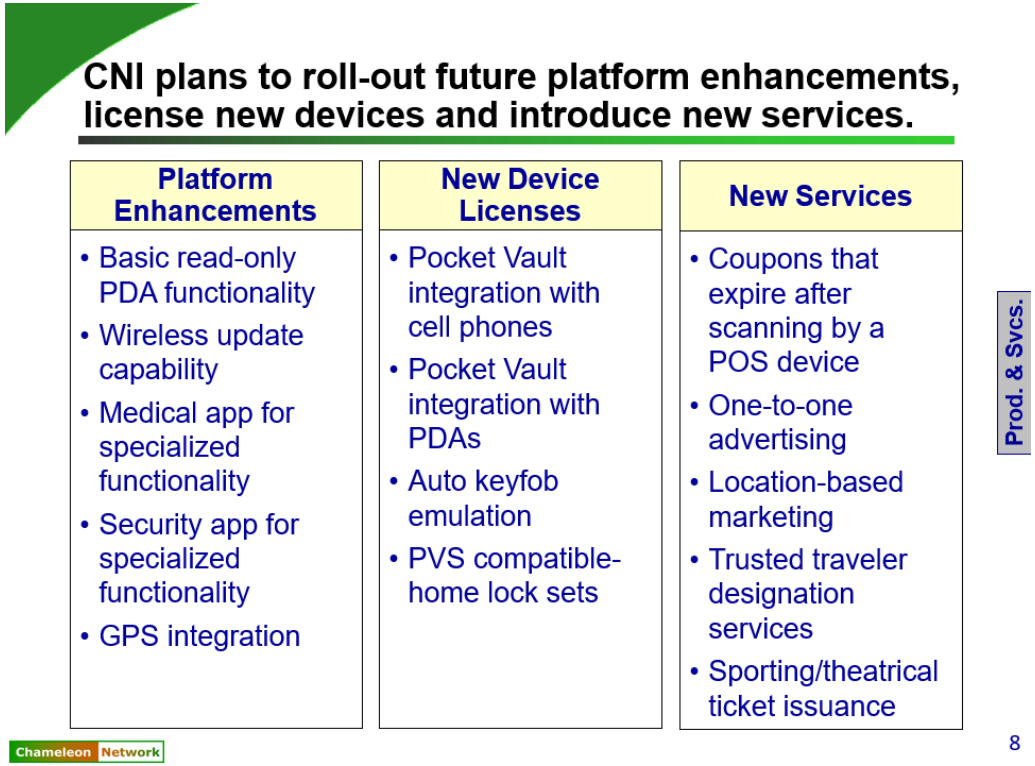
Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id.* at 4.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandiz ing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault



TFrab at 8.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

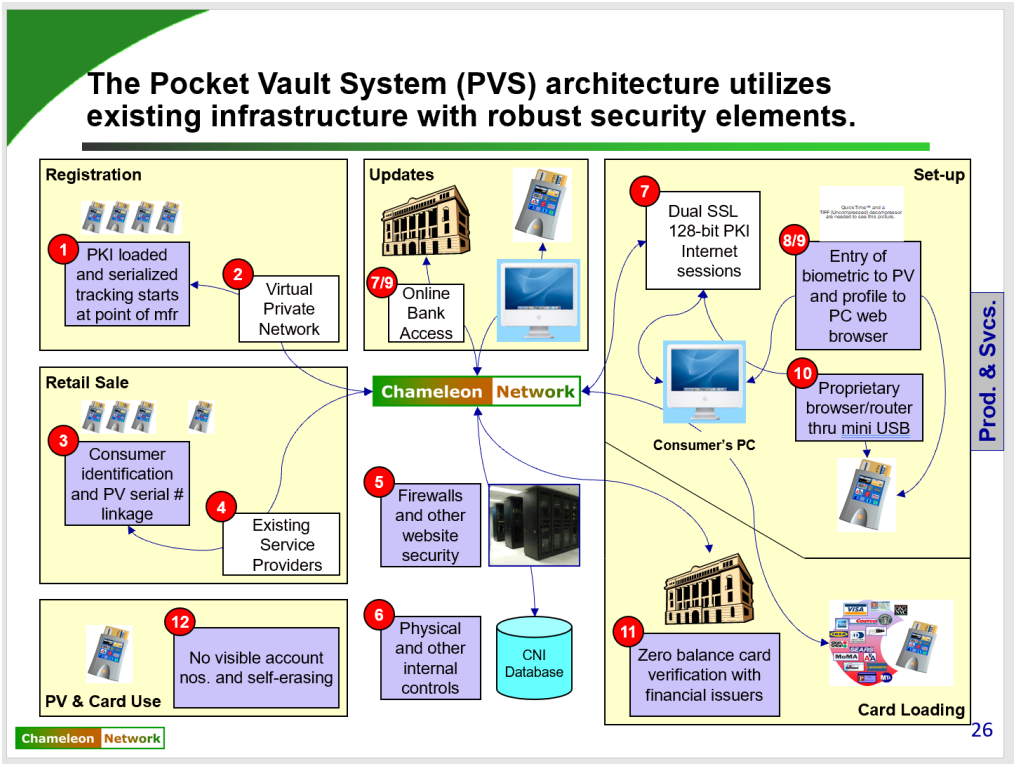
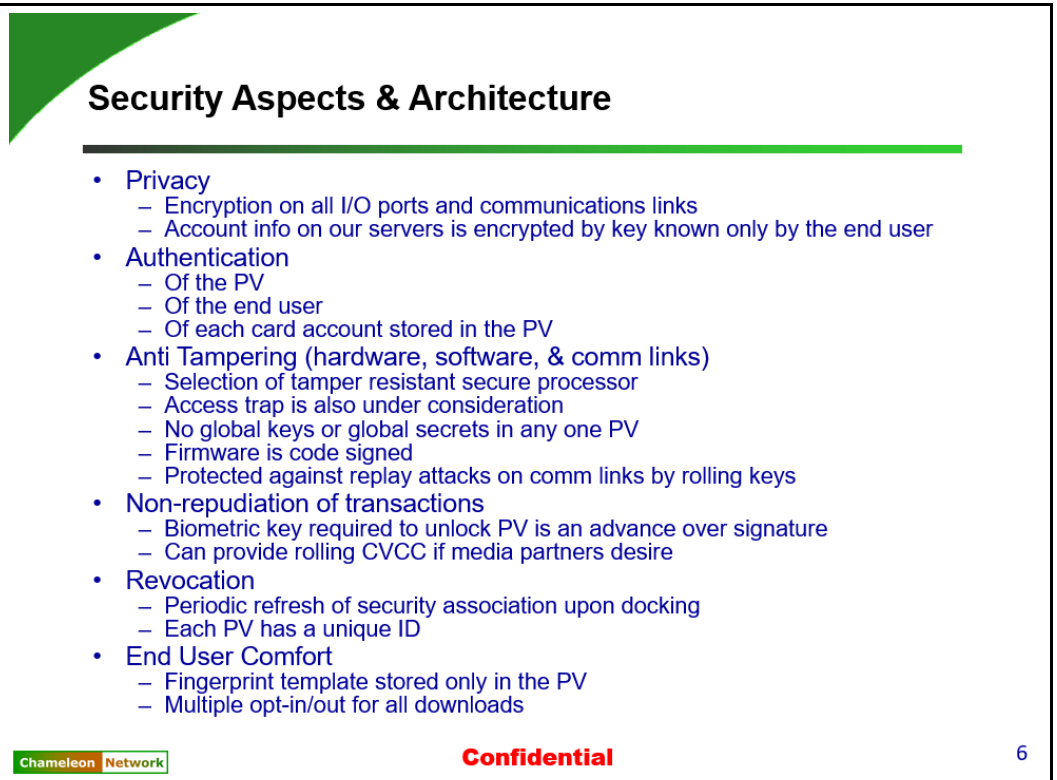
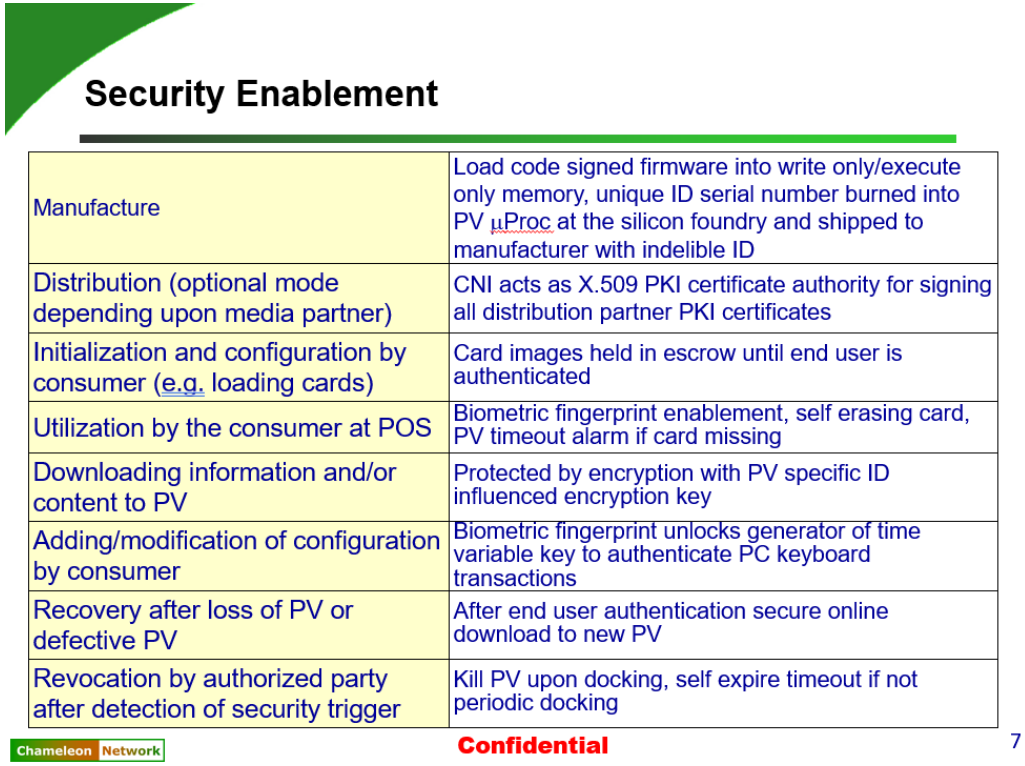
		 TFrab at 26.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault



Sec3 at 6.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 7.
</td>
</tr>
<tr>
<td>1G</td>
<td>allowing the user to complete a financial transaction.</td>
<td>Pocket Vault discloses allowing the user to complete a financial transaction.

For example, Pocket Vault discloses use of the system to complete a credit card transaction or create hotel room key cards to access hotel rooms.

See, e.g.,

“The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various financial and non-financial media, that also may enable individuals and retailers</td>
</tr>
</table>

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns." *Burger* at [0095]. "One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time-sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who intake room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104 b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room." *Burger* at [0676].

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"As shown, the routine 1400 begins at a step 1402, wherein a menu is displayed on the display 324 of the interface station computer 304 that gives the operator of the interface station computer 304 several options to choose from. These options may, for example, include: (1) the option to request that a Pocket Vault 102 be validated (i.e., permitted to store a new finger print), (2) the option to request that the information currently stored on a Pocket Vault 102 be updated (e.g., information may be uploaded from the network server 114), (3) the option to request that a transaction involving a Pocket Vault 102 be authorized, and/or (4) the option to access a website on the network server 114 and take advantage of the functionality thereof." *Burger* at [0365] "Customer use a. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. b. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		• The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. Pocket Vault Overview *Pocket Vault System* replaces a consumer's conventional wallet and stores an entire wallet's contents in digital form (credit, ATM, identification, physical and network access, membership, discount cards), in a stand-alone device or integrated into PDAs and mobile phones. The Pocket Vault programs a single, "morphing" Chameleon Card to emulate the characteristics of any magnetic stripe, barcode or smart card that the user selects. The Pocket Vault and Chameleon Card are useable everywhere (brick & mortar and online), and are completely compatible with all existing point-of-sale terminals. Pocket Vault Overview.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.
4	The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris Scan, a hand geometry, a facial recognition, a signature recognition and a Voice recognition.	Pocket Vault discloses the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris Scan, a hand geometry, a facial recognition, a signature recognition and a Voice recognition. Pocket Vault discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition. *See, e.g.,*

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		"In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in FIG. 2." "As discussed below in more detail, in some embodiments of the invention, certain uses of the Pocket Vault 102, as well as each of the interface stations 104 a-c, may be permitted only by pre-authorized individuals. To this end, a suitable user authentication technique may be employed in connection with each attempted use of any of these devices. One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis. Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder's identity. In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly." *Burger* at [0112].

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandiz ing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "The biometric information is stored in a secure, tamper-resistant component of the POCKET VAULT and is not stored in the Pocket Vault System." Service Definition at 5.4.2.1. Initialize Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer; o Enroll at least two fingerprints to the device; o Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time."

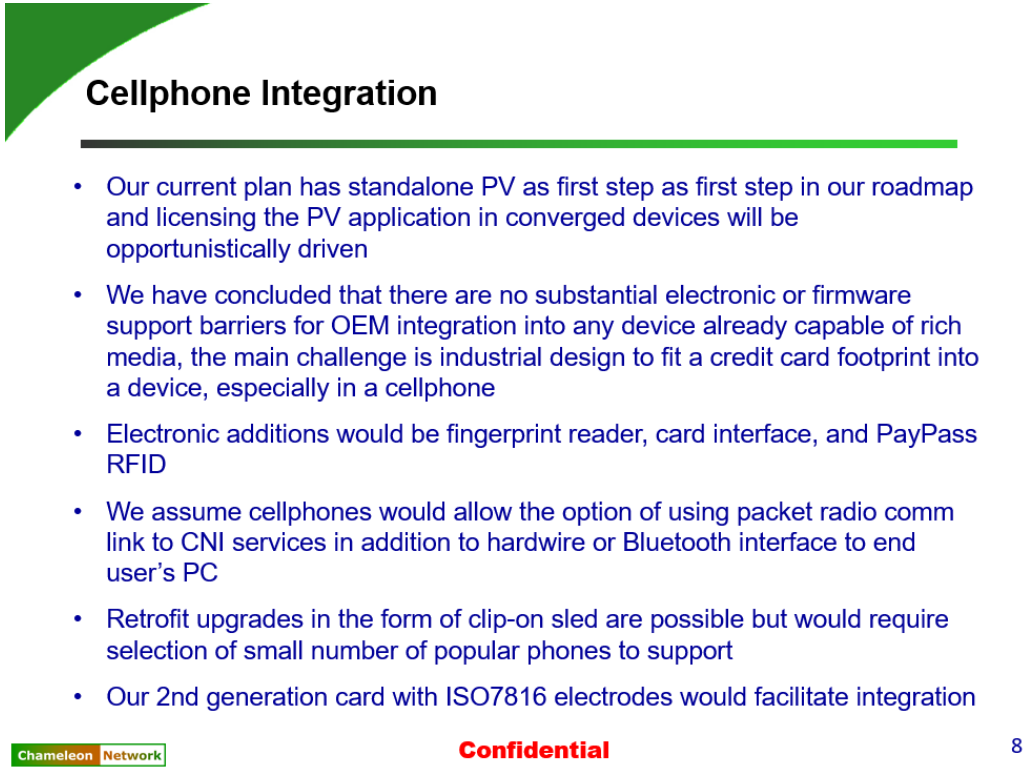
Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		Spec Tob at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." Service Definition at 10-11. TFrab at 26.
5	The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player,	To the extent that this element is not explicitly disclosed by *Pocket Vault*, a POSITA would have found it obvious in light of this reference. A POSITA would have been motivated to combine the teachings of this reference with the knowledge of a person of ordinary skill in the art, and/or combine this reference

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

	mobile gaming device, watch and a key fob.	with the other references charted for this patent in these Invalidity Contentions. For example, one of skill in the art would find the combination obvious to try, due at least to the similarity of the technical teachings of the art. As another example, one of skill in the art would find that the teachings could be predictably interchanged by, for example, simple substitution, at least because of the predictability of the art and the known interchangeability of the various elements. As another example, one of skill in the art would be motivated to combine the references, and would have a reasonable expectation of success in doing so, at least because the references use known variations of existing technology to solve routine and well understood problems in predictable ways. Further motivations to combine references and additional details may be found in the Cover Pleading.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault



Sec3 at 8.

"Innovations in Palm Computing
There are a number of ongoing developments in the palm computing arena that could be important to Chameleon Network. The integration of secure wireless connections through companies like Symbian tighten the potential links with purchasing transactions. "Digital signatures" create a more secure transaction over the wireless application protocol (WAP) usage. This is part of the "smart phone" clash. Additional breakthroughs linking palm computing and fingerprint/voice/retinal identification will compete to provide more secure transactions, and could be part of a smart phone market play as well."
CNIFullBizPln at 34.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

7	The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.	Pocket Vault discloses completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account. *See* 1G.
9pre	An integrated device comprising:	Pocket Vault discloses an integrated device. *See* 1pre.
9A	a persistent storage media that persistently stores biometric data of a user and an ID code;	Pocket Vault discloses a persistent storage media that persistently stores biometric data of a user and an ID code. *See* IA.
9B	a validation module, coupled to communicate with the persistent storage media,	Pocket Vault discloses a validation module, coupled to communicate with the persistent storage media, *See* 1B-1C.
9C	that receives scan data from a biometric scan for comparison against the biometric data,	Pocket Vault discloses receiving scan data from a biometric scan for comparison against the biometric data. *See* 1B-1C.
9D	and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and	Pocket Vault discloses sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. *See* 1E.
9E	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that	Pocket Vault discloses a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority Successfully authenticated the ID code sent to the

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

	the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and	third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction. *See* 1E.
9F	allowing the user to-complete a financial transaction.	Pocket Vault discloses allowing the user to-complete a financial transaction. *See* 1F For example, Pocket Vault discloses an encrypted transaction approval message. *See, e.g.,* "When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID. After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732. When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed." *Burger* at [0437]-[0439]

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		Pocket Vault Overview *Pocket Vault System* replaces a consumer's conventional wallet and stores an entire wallet's contents in digital form (credit, ATM, identification, physical and network access, membership, discount cards), in a stand-alone device or integrated into PDAs and mobile phones. The Pocket Vault programs a single, "morphing" Chameleon Card to emulate the characteristics of any magnetic stripe, barcode or smart card that the user selects. The Pocket Vault and Chameleon Card are useable everywhere (brick & mortar and online), and are completely compatible with all existing point-of-sale terminals. Pocket Vault Overview. "Customer use c. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.)

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. d. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6.
10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.	Pocket Vault discloses the ID code is transmitted to the third-party trusted authority over a network. For example, Pocket Vault discloses communications with a network server. *See, e.g.*, "The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various financial and non-financial media, that also may enable individuals and retailers to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns." *Burger* at [0095]. "When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304." *Burger* at [0349]. "According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus." *Burger* at [0019]. "When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device." *Burger* at [0186]. "When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." Service Definition at 22. "Customer use e. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault

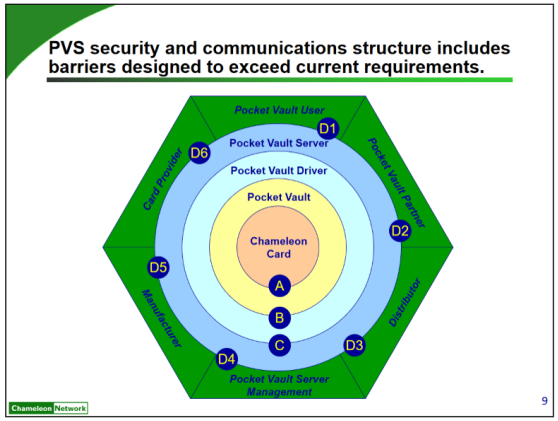
Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

		3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. f. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


<table>
<tr><th>Barrier</th><th>Technologies</th></tr>
<tr><td>A</td><td>Encryption, bi-directional authentication, EMV standards</td></tr>
<tr><td>B</td><td>https/SSL, PKI, authentication, physical connection</td></tr>
<tr><td>C</td><td>https/SSL, authentication, firewall, PKI</td></tr>
<tr><td>D*</td><td>Authentication, https/SSL, firewall</td></tr>
<tr><td>D1</td><td>Requires PV session (B+C)</td></tr>
<tr><td>D2</td><td>VPN, PKI</td></tr>
<tr><td>D3</td><td>Post only commands</td></tr>
<tr><td>D4</td><td>VPN, PKI</td></tr>
<tr><td>D5</td><td>VPN, PKI</td></tr>
<tr><td>D6</td><td>VPN, PKI</td></tr>
<tr><th>Component</th><th>Technologies</th></tr>
<tr><td>CN Card</td><td>Card registration, auto-erase</td></tr>
<tr><td>PV commands</td><td>Tamper-resistant components, fingerprint, fixed set of allowable</td></tr>
<tr><td>PV Driver</td><td>Trusted USB driver/router</td></tr>
<tr><td>PVS</td><td>Isolated subnet for database, fixed set of allowable commands</td></tr>
</table>
Visa Intl at 9.
</td>
</tr>
<tr>
<td>12</td>
<td>The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop,</td>
<td>Pocket Vault discloses the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

See 5.</td>
</tr>
</table>

Exhibit 905-L
Invalidity Chart for U.S. Patent No. 9,289,905 In View of Pocket Vault

	mp3 player, mobile gaming device, watch and a key fob.	

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

The Pocket Vault System ("Pocket Vault") was in public use, on sale, sold, known in this country, or otherwise available to the public before the priority date of U.S. Pat. No. 10,689,989 ("the '989 Patent"). Features of Pocket Vault would have been apparent to a person of ordinary skill in the art using the public system, rendering the system § 102(a), (b), and/or (g) prior art. [1]

At least the following documents, or the documents referenced therein, describe the functionality of Pocket Vault:

- https://web.archive.org/web/20040602202951/http://chameleonnetwork.com/pocket_vault_info.htm ("Pocket Vault Overview")
- https://web.archive.org/web/20040529034458/http://www.chameleonnetwork.com/Articles/StrategicFinance/SF%20Comp%20v3.pdf ("Out of Pocket")
- https://web.archive.org/web/20040603023030/http://www.wired.com/news/business/0,1367,62545,00.html?tw=wn_tophead_7 ("Changes Stripes")
- U.S. Patent Application Publication No. 2003/0220876 ("Burger")
- PV Service Definition v0_12 ("Service Definition")
- Provisioning Overview ("Overview")
- Marzen Team Pro…11 Mar 2002 copy ("Marzen")
- pocket vault spec_tob copy.doc ("Spec Tob")

[1] Samsung notes that Plaintiff appears in many instances to be pursuing overly broad constructions of various limitations of the asserted claims of the '989 Patent in an effort to piece together an infringement claim where none exists and to accuse a product that does not practice the claims. This claim chart may take into account Plaintiff's overly broad constructions of the claim limitations. Any assertion that a particular limitation is disclosed by a prior art reference may be based on Plaintiff's apparent constructions and is not intended to be, and is not, an admission that such constructions are supportable or proper.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

- TFarb VC CNI 101404 copy ("TFarb")
- sec3.ppt ("Sec3")
- CitiCNI mtg 120601 Q&A ("CitiCNI")
- Visa Intl Tech Mtg 1204 v3 ("Visa Intl")
- Brookstone FAQ v4 ("Brookstone")

To the extent Plaintiff alleges that Pocket Vault does not disclose any particular limitation of the Asserted Claims of the '989 Patent, either expressly or inherently, it would have been obvious to a person of ordinary skill in the art as of the priority date of the '989 Patent to modify the Pocket Vault reference and/or to combine the teachings of the Pocket Vault reference with other prior art references, including but not limited to the present prior art references found in Exhibit 989-A-K and 989-M-R and the corresponding section(s) of charts for other prior art references for the '989 Patent in a manner that would have rendered the Asserted Claims invalid as obvious.

With respect to the obviousness of the Asserted Claims under 35 U.S.C. § 103, one or more of the principles enumerated by the United States Supreme Court in *KSR v. Teleflex*, 550 U.S. 398 (2007) apply, including: (a) combining various claimed elements known in the prior art according to known methods to yield a predictable result; and/or (b) making a simple substitution of one or more known elements for another to obtain a predictable result; and/or (c) using a known technique to improve a similar device or method in the same way; and/or (d) applying a known technique to a known device or method ready for improvement to yield a predictable result; and/or (e) choosing from a finite number of identified, predictable solutions with a reasonable expectation of success or, in other words, the solution was one which was "obvious to try"; and/or (f) a known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on given design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and/or (g) a teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention. It therefore would have been obvious to one of ordinary skill in the art to combine the disclosures of these references in accordance with the principles and rationales set forth above.

The citations to portions of any reference in this chart are exemplary only. For example, a citation that refers to or discusses a figure or figure item should be understood to also incorporate by reference that figure and any additional descriptions of that figure as if set forth fully therein. Samsung reserves the right to rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid. Citations presented for one claim limitation are expressly incorporated by reference into all other limitations for

that claim as well as all limitations of all claims on which that claim depends. Samsung also reserves the right to rely on additional citations or sources of evidence that also may be applicable, or that may become applicable in light of claim construction, changes in Plaintiff's infringement contentions, and/or information obtained during discovery as the case progresses.

Claim	U.S. Patent No. 10,689,989	Exemplary Disclosure in Pocket Vault
1pre	A method comprising:	Pocket Vault discloses a method. For example, Pocket Vault discloses verification using biometric data through a device. *See, e.g.,* "According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user." *Burger* at[0007]. "According to another aspect, a method for using an apparatus comprises steps of using the apparatus to authenticate an identity of a user of the apparatus, and after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal." *Burger* at [0010]. for Consumers • financial, discount and affinity cards aggregated in one place, with complete security • secure backup and instant replacement of all wallet contents • current account status for debit, credit, identity and membership cards • promotions, coupons and discount offers delivered into consumers' "wallets" and available for use at point of purchase

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		Pocket Vault Overview.
1A	receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;	Pocket Vault discloses receiving, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the device among a plurality of devices. For example, Pocket Vault discloses receive a unique ID code and storing fingerprint information in persistent, tamper proof "write-once memory 212." *Burger* [0182]. Burger also discloses "a unique encrypted chip ID." *Burger* at [0114]. *See, e.g.,* "After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. In one embodiment, the Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of FIG. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114, as described below." *Burger* At [0182].

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

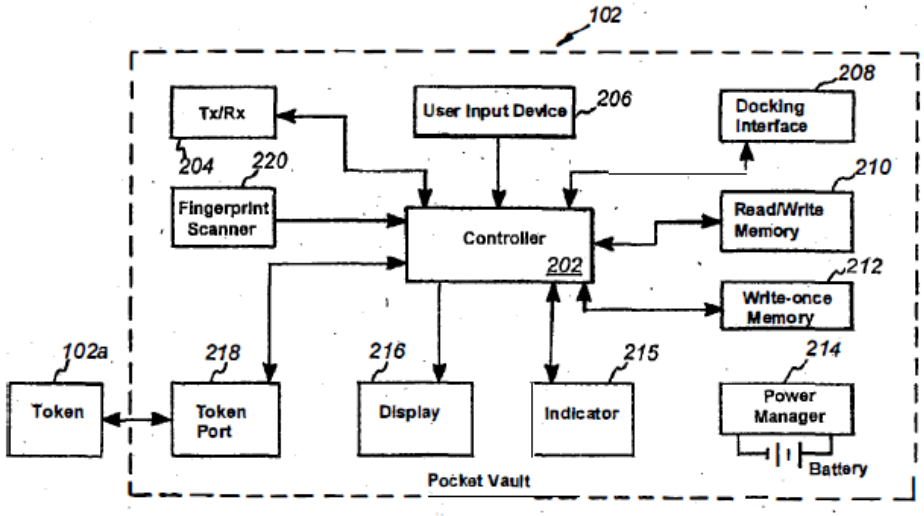


Fig. 2

"As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information." *Burger* at [0114].

"Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault 102, and the entire contents of the lost Pocket

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card." *Burger* at [0116]. for Card Issuers • Issuer becomes "portal" to customers' entire wallet contents • powerful new marketing and loyalty tools • takes customer relationships to dynamic new levels • significant reductions in fraud & operations costs for Employers • secure and centralized issuance, administration and retrieval of ID and access-control cards • supports multiple ID systems and multiple access control devices • consolidates multiple employer-issued cards onto single Pocket Vault Overview.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket. "The biometric information is stored in a secure, tamper-resistant component of the POCKET VAULT and is not stored in the Pocket Vault System." *Service Definition* at 5.4.2.1. Initialize Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer;

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		○ Enroll at least two fingerprints to the device; ○ Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." *Id*. at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

- Use a unique or random encryption method that makes each wallet different from others.
- Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet.
- Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear.
- Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code."

Id. at 10-11.

10.11.1 PV Configuration Data Dictionary

Attribute	Definition
ID	This is an internal identifier that is unique within this instantiation of the ***Pocket Vault System***.
Status	This is the current status. • `WIP`: Partially created, but not ready for use • `Active`: Fully created and ready for use. • `Inactive`: The **PV CONFIGURATION** is no longer used and can be purged from the system.
Name	This is the Name of the **PV CONFIGURATION**.
Start Date	This is the date the **PV CONFIGURATION** was created.
End Date	This is the date the **PV CONFIGURATION** is no longer in use.
Time-out Period	The amount of time, in minutes, before the **POCKET VAULT** goes to the `Locked` Status which prevents further activity without reauthentication.
▶	

Id. at 68.

"Register Pocket Vault

This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id*. at 4. "Customer use a. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. b. Financial transactions – When using the Pocket Vault for financial transactions the consumer:

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

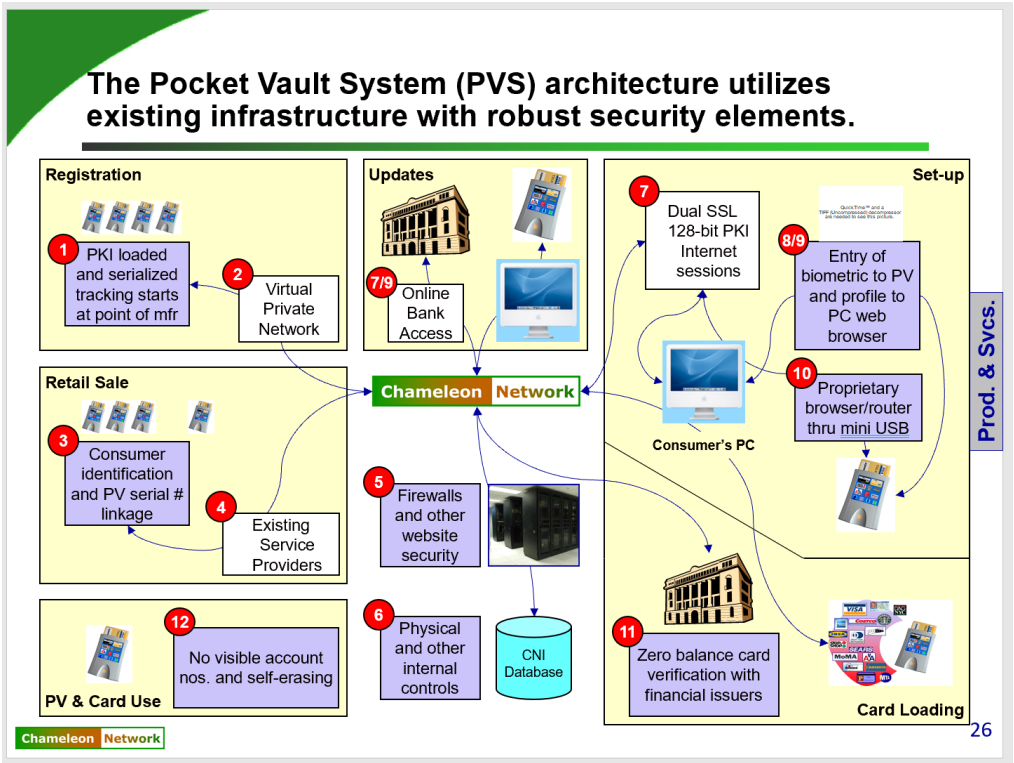
		 TFarb at 26.
1B	persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;	Pocket Vault discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition. See 1A. Pocket Vault discloses wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition. *See, e.g.*,

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in FIG. 2." *Burger* at [0107]. "As discussed below in more detail, in some embodiments of the invention, certain uses of the Pocket Vault 102, as well as each of the interface stations 104 a-c, may be permitted only by pre-authorized individuals. To this end, a suitable user authentication technique may be employed in connection with each attempted use of any of these devices. One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis. Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder's identity. In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly." *Burger* at [0112].

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "The biometric information is stored in a secure, tamper-resistant component of the POCKET VAULT and is not stored in the Pocket Vault System." *Service Definition* at 5.4.2.1. Initialize Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer; o Enroll at least two fingerprints to the device; o Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." Service Definition at 10-11.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

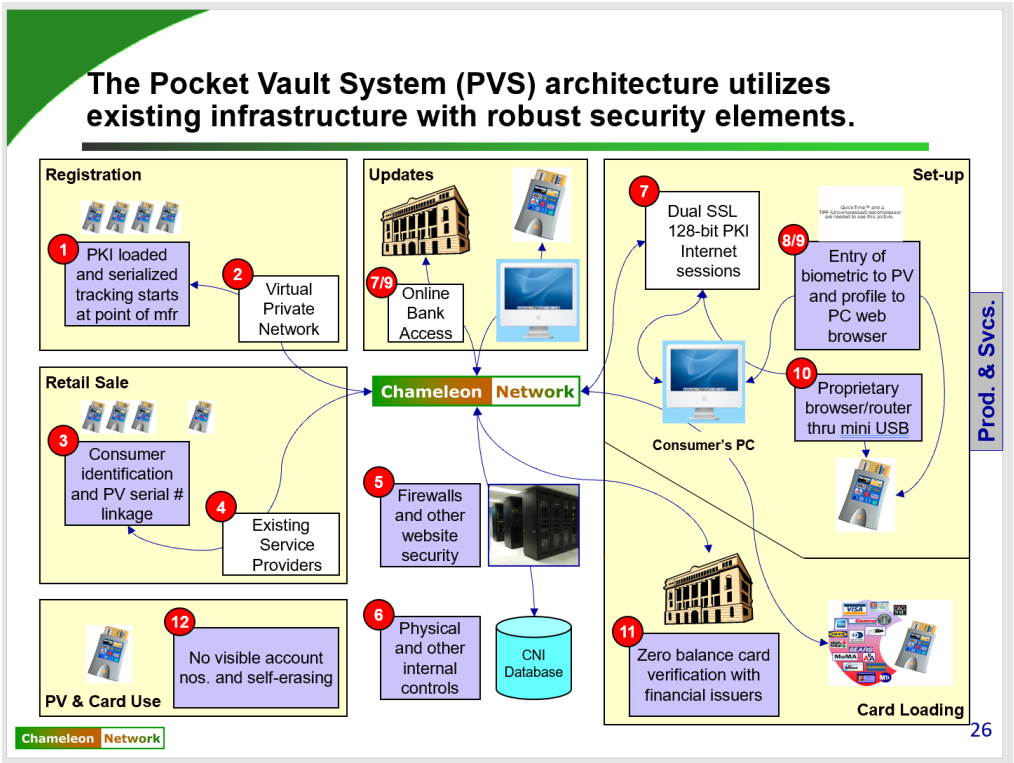
		 TFrab at 26.
1C	receiving, at the smartphone, scan data from a biometric scan using the smartphone;	Pocket Vault discloses responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan. For example, Pocket Vault discloses scanning a user fingerprint when user's finger is placed on a biometric sensor. *See, e.g.*, "When, at the step 1302, it is determined that a first encrypted message including a Pocket Vault ID has been received from the Pocket Vault 102, the

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		routine 1300 proceeds to a step 1304, wherein the first encrypted message is forwarded to the interface station computer 304 (FIG. 3) After the step 1304, the routine 1300 proceeds to steps 1306 and 1308, wherein it is determined whether a fingerprint has been scanned by the fingerprint scanner 316 of the pocket vault interface unit 302 before a timeout period measured by the step 1308 has elapsed. When, at the steps 1306 and 1308, it is determined that a fingerprint has not been scanned within the timeout period of step 1308, the routine 1300 returns to the step 1346 (discussed above). When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302." *Burger* at [0345]-[0348].

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

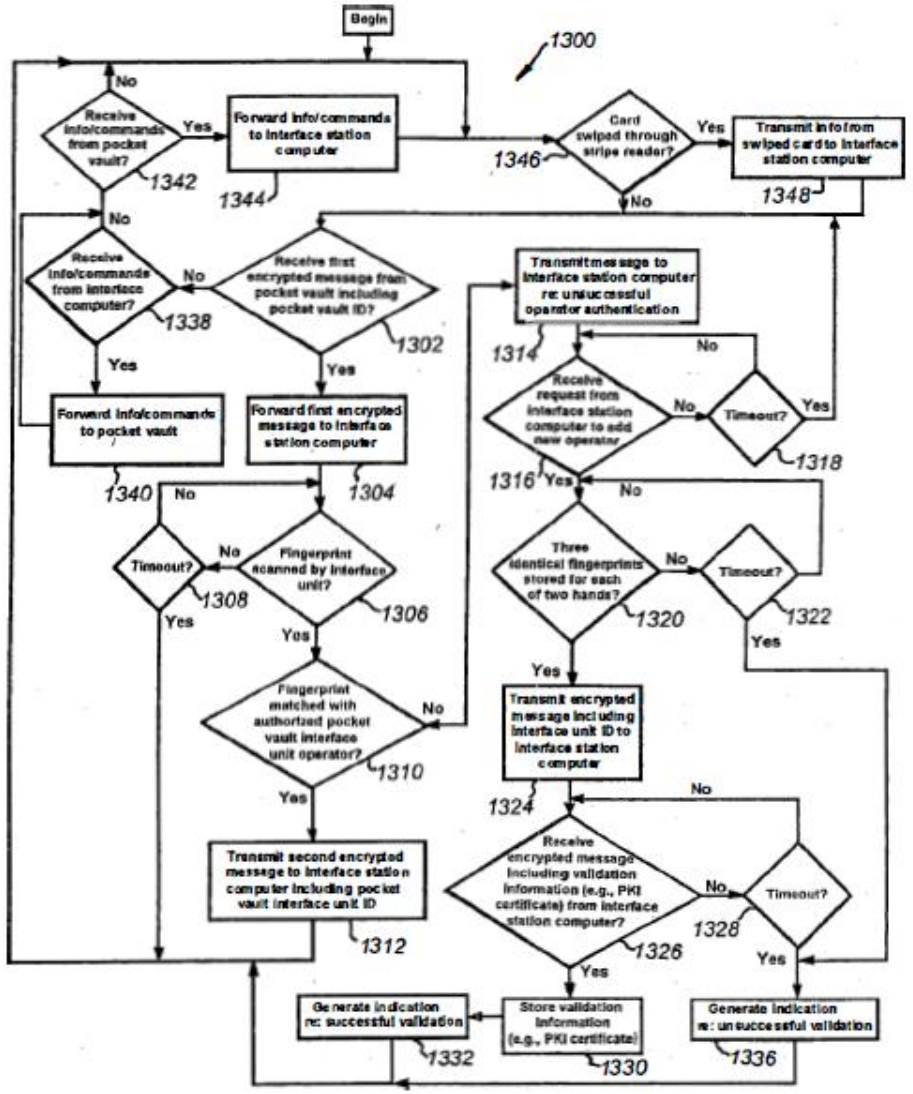


Fig. 13

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"As shown, the routine 3024 begins at a step 3302, wherein it is determined whether the Pocket Vault 102 has been authenticated, e.g., whether the Pocket Vault 102 has determined that a fingerprint applied to the fingerprint scanner 220 matches one of the fingerprints stored in the fingerprint memory of the Pocket Vault 102. This authentication procedure may operate as described above in connection with the step 712 (FIG. 7), or an additional or different routine may be employed (e.g., as part of the security module 2812 described above in connection with FIG. 28) to determine whether the holder has successfully authenticated his or her identity, thereby enabling the network server 114 to establish a "trust" relationship with the Pocket Vault 102." *Burger* at [0595].

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." *Service Definition* at 5.5.1.2.1. Unlock Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer; o Enroll at least two fingerprints to the device; o Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

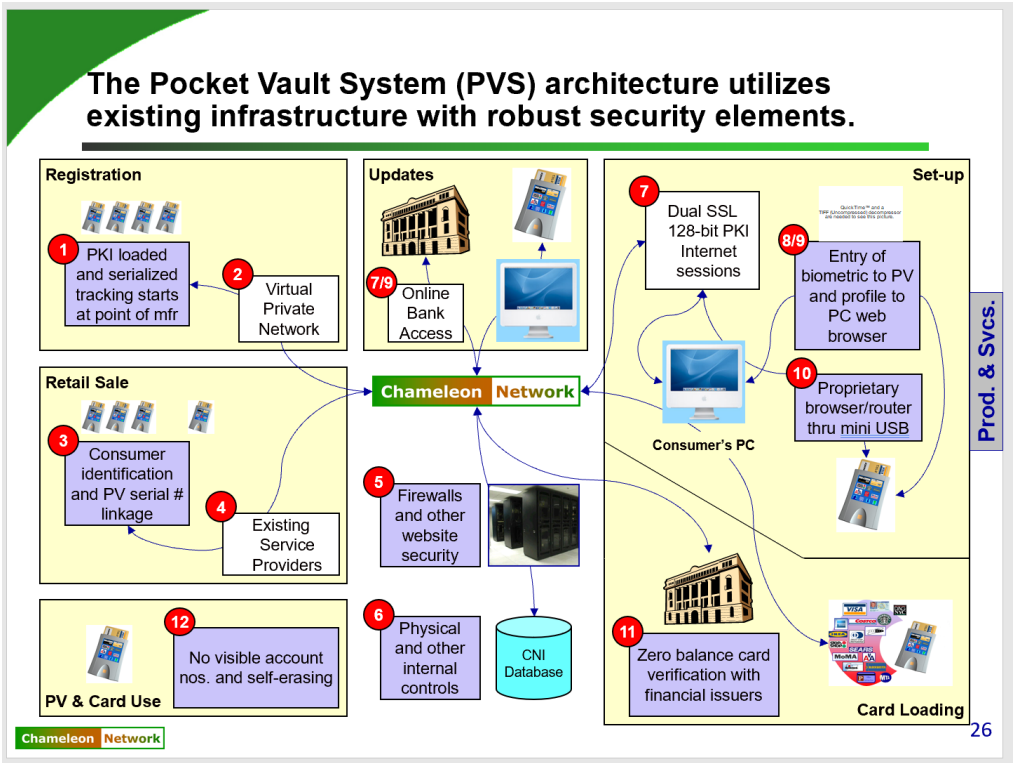
		 TFrab at 26.
1D	comparing, using the smartphone, the scan data to the biometric data;	Pocket Vault discloses comparing the scan data to the biometric data to determine whether the scan data matches the biometric data. For example, Pocket Vault discloses comparing the fingerprint image with the fingerprint template. *See, e.g.*, "When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302." *Burger* at [0348]. "When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212." *Burger* at [0184]. "When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (FIG. 7) matches one of the stored fingerprints." *Burger* at [0209]. "After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match)." *Burger* at [0336]. First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		Changes Stripes. "…use fingerprint match; if successful, display initial screen; change status from Locked to Unlocked." *Service Definition* at 5.5.1.2.1. Unlock Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer; o Enroll at least two fingerprints to the device; o Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11. "Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.
1E	determining whether the scan data matches the biometric data; and	Pocket Vault discloses responsive to a determining whether the scan data matches the biometric data. *See* 1D.
1F	responsive to a determination that the scan data matches the biometric data	Pocket Vault discloses responsive to a determination that the scan data matches the biometric data. *See* 1D.
1G	wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority	Pocket Vault discloses wirelessly sending, from the device, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. For example, Pocket Vault discloses transmitting a second encrypted message including an ID of the pocket vault interface to the interface station computer. *See, e.g.,* "According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user." *Burger* at[0007]. "When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304." *Burger* at [0349]. "According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus." *Burger* at [0019]. "When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device." *Burger* at [0186]. "When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. "When, at the step 2306, it is determined that the secure media issuer is a Pocket Vault participant, the routine 1918 proceeds to a step 2310, wherein the media issuer is queried as to the account status of the holder. After the step 2310, the routine 1918 proceeds to a step 2312, wherein it is determined whether authorization has been received from the media issuer to load the file."

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		Burger at [0506]. When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (FIG. 4). As shown, the logged information may include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction. After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107). *Burger* at [0516]-[0518]. When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the Pocket Vault ID (if available) is linked to the ID of the entity proposing the transaction, e.g., a commercial interface station 104 c, a card reader 106, a barcode reader 107, or an RFID interrogator 107. *Burger* at [0526]. After the step 3410, the routine proceeds to a step 3412, wherein the website on the network server 114 determines whether the account for the card is valid. This determination may be made, for example, by confirming that the card is owned by the person attempting to add it to his or her Pocket Vault 102, that the card has not expired, etc. *Burger* at [0620]. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID;

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		• The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id.* at 22. "5.4.1.2.4 Establish Wireless Pocket Vault Session A PV User or PV Manager can receive updates even when not docked to a PC. This subprocess can only be initiated after successful completion of the Unlock Pocket Vault subprocess. The PV User or PV Manager navigates to the POCKET VAULT icon to start the wireless session. • Request Update / Set session timeout • Establish secure PV to Pocket Vault System session

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

• Initiate Update Pocket Vault process"
Id. at 41.

10.11.1 PV Configuration Data Dictionary

Attribute	Definition
ID	This is an internal identifier that is unique within this instantiation of the ***Pocket Vault System***.
Status	This is the current status. • `WIP`: Partially created, but not ready for use • `Active`: Fully created and ready for use. • `Inactive`: The **PV CONFIGURATION** is no longer used and can be purged from the system.
Name	This is the Name of the **PV CONFIGURATION**.
Start Date	This is the date the **PV CONFIGURATION** was created.
End Date	This is the date the **PV CONFIGURATION** is no longer in use.
Time-out Period	The amount of time, in minutes, before the **POCKET VAULT** goes to the `Locked` Status which prevents further activity without reauthentication.
►	

Id. at 68.

"The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond."
Spec Tob at 5.

"To do this, the wallet must do at least the following:
- Store all credit card and fingerprint information in an encrypted form.
- Use a unique or random encryption method that makes each wallet different from others.
- Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		□ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id*. at 10-11. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer. • The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id.* at 4. "Customer use c. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website

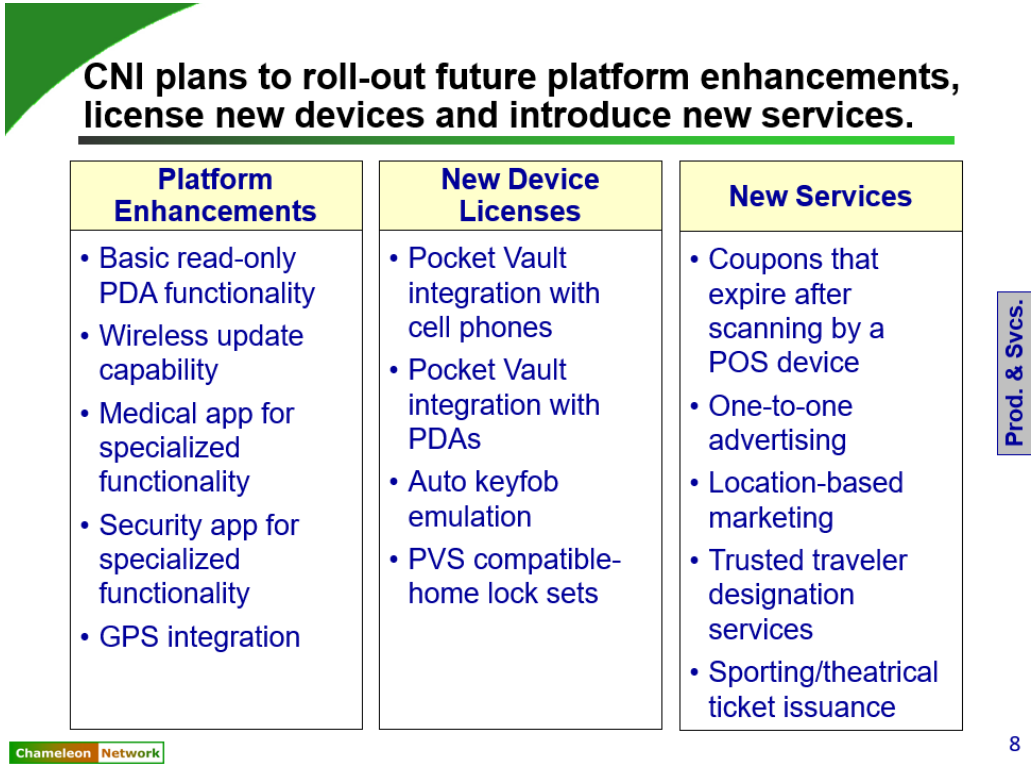
Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. d. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandiz ing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



TFrab at 8.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

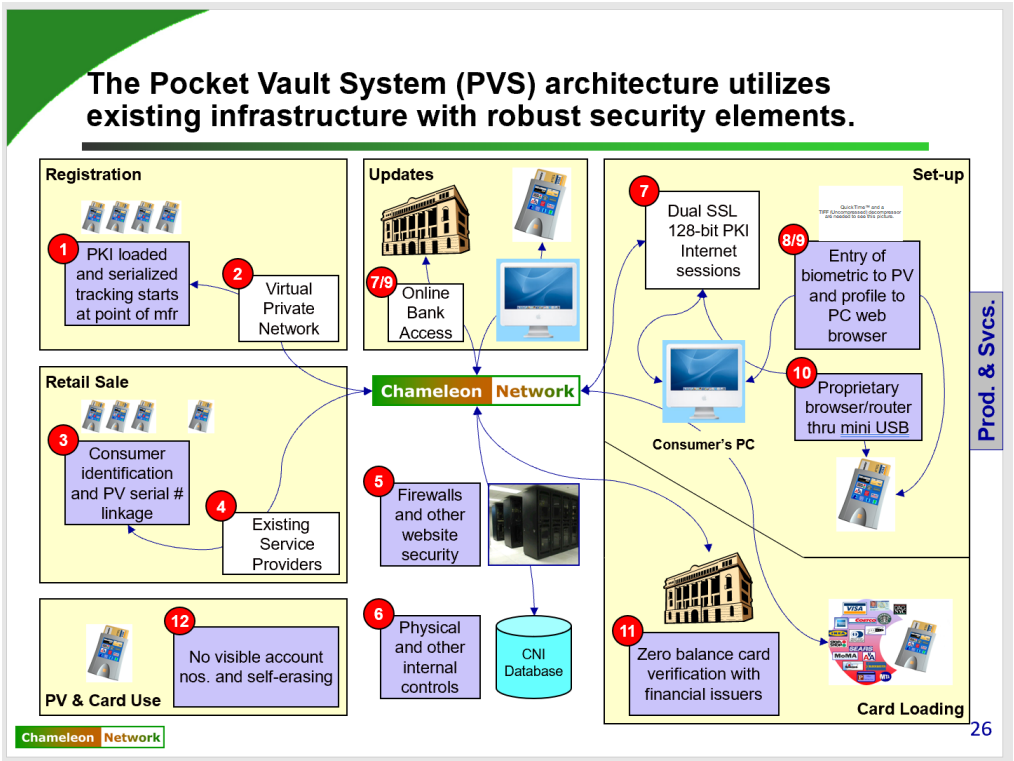
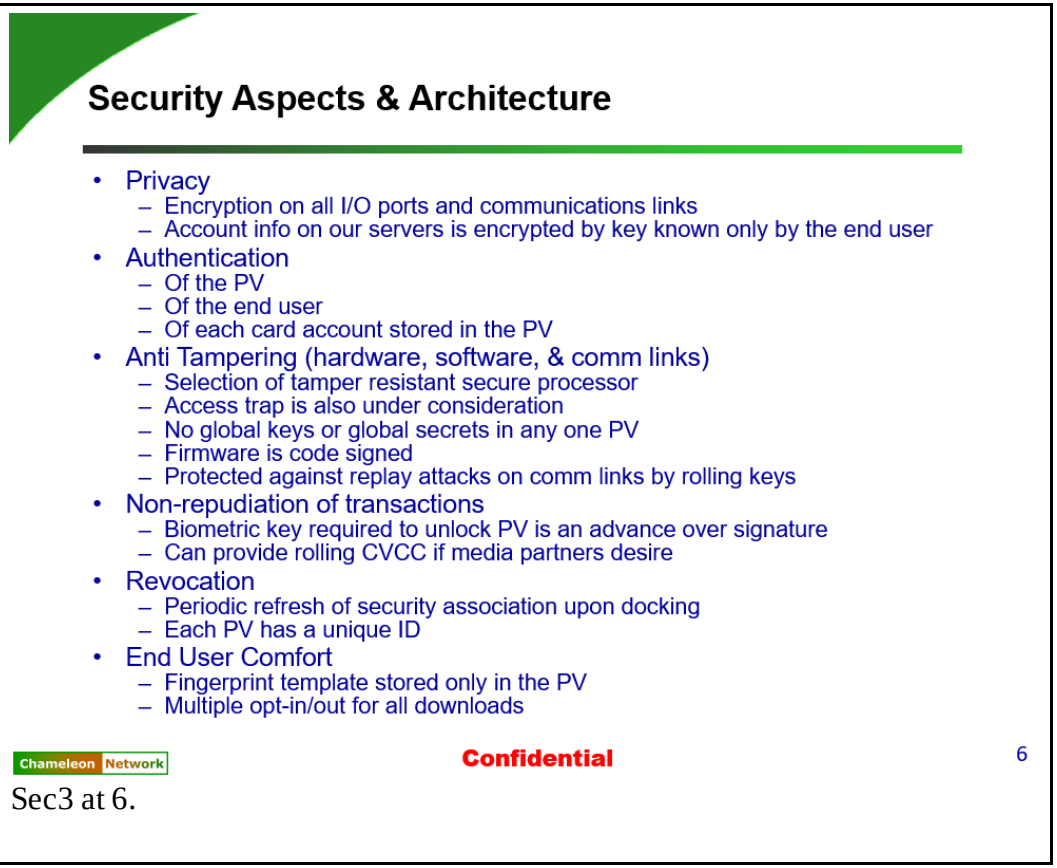
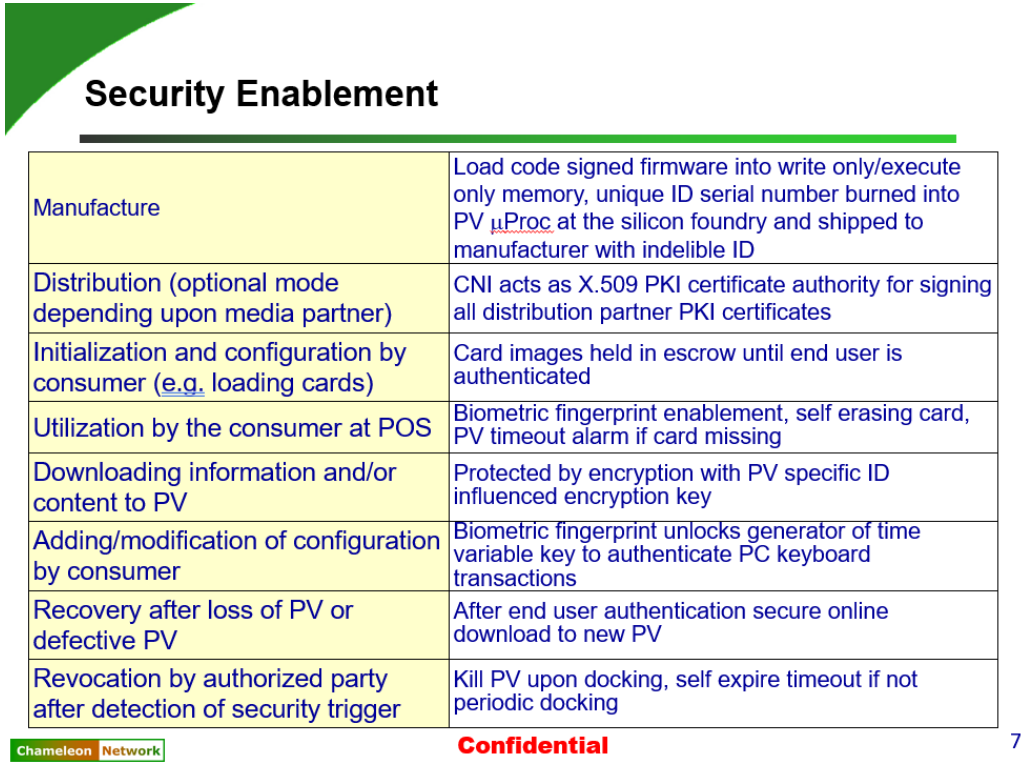
		 TFrab at 26.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 6.
</td>
</tr>
</table>

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 7.</td>
</tr>
<tr>
<td>1H</td>
<td>a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code</td>
<td>Pocket Vault discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code.

For example, Pocket Vault discloses making a determination whether a Pocket Vault ID is valid and sending an encrypted transaction approval message

See, e.g.,

“When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is</td>
</tr>
</table>

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. "When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID. After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732. When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed." *Burger* at [0437]-[0439] Pocket Vault Overview *Pocket Vault System* replaces a consumer's conventional wallet and stores an entire wallet's contents in digital form (credit, ATM, identification, physical and network access, membership, discount cards), in a stand-alone device or integrated into PDAs and mobile phones. The Pocket Vault programs a single, "morphing" Chameleon Card to emulate the characteristics of any magnetic stripe, barcode or smart card that the user selects. The Pocket Vault and Chameleon Card are useable everywhere (brick & mortar and online), and are completely compatible with all existing point-of-sale terminals. Pocket Vault Overview. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and • The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id*. at 22. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others. □ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id*. at 10-11. "Register Pocket Vault This subprocess is initiated by the consumer. The consumer is prompted to enter basic Pocket Vault account and security info which is linked to Pocket Vault ID on Pocket Vault System. Because there is no point-of-sale information linking the Pocket Vault to the consumer, additional steps are taken to ensure that the consumer is who they claim to be. These steps may include, but are not limited to the following. These steps can only be done from the consumer's home. • The consumer is required to provide their name, home address, and home telephone number. • The consumer is required to provide a major credit card from a US-based issuer. Using standard retail credit card transactions available in the POS network, we verify that the name and address information for the credit card match the information provided by the consumer. • The consumer is requested to provide a home telephone number listed in the consumer's name. Using reverse telephone number lookup (via commercially available web services), we verify that the name and address associated with the telephone number is the same as that provided by the consumer.

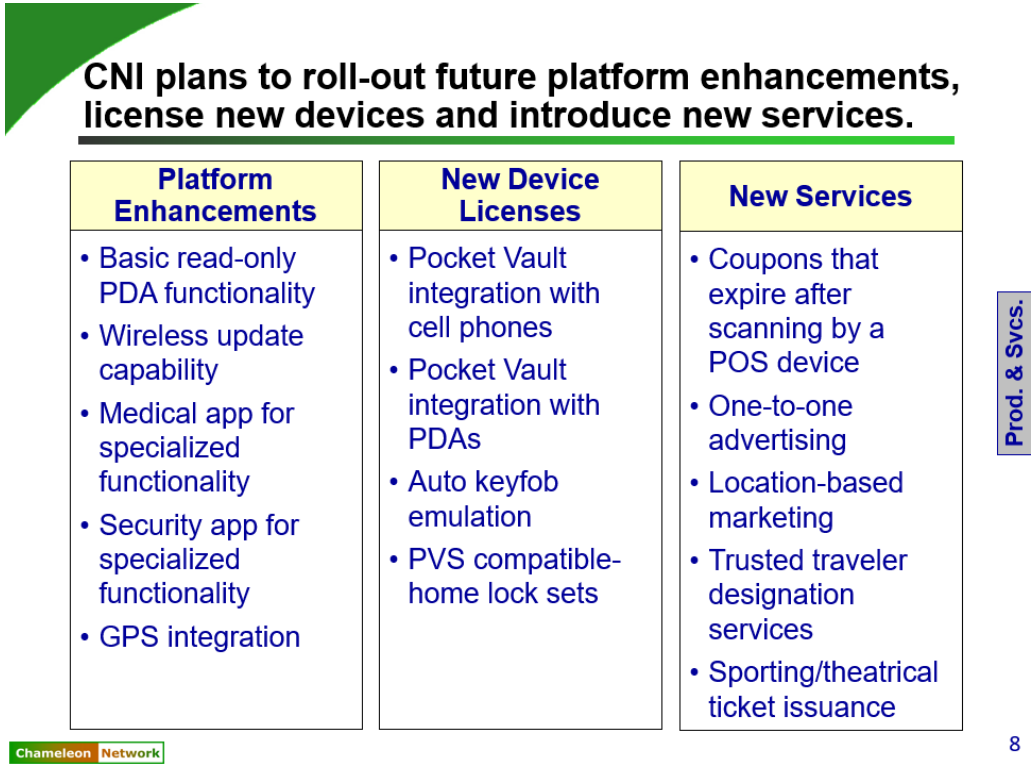
Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		• The consumer is requested to call a toll-free number. Using ANI, we confirm that the number is the same as that provided by the consumer. To help prevent automated attacks, the consumer is required to enter, on the telephone handset, the numeric value that is displayed in the browser as an image. • We use the IP address (via commercially available web services) to verify that the consumer's ISP is in the same geographic vicinity as the home address. The Pocket Vault System validates identification information against information from external sources before allowing the consumer to complete the initialization. The remainder of the process is the same as in Initialize Pocket Vault." Overview at 5-6. "Remove Pocket Vault This subprocess is used by the reseller to prevent a Pocket Vault from ever being used again. The subprocess is used when the Pocket Vault is damaged, stolen, or misplaced. The Pocket Vault System keeps track of the Pocket Vault ID and changes its status to one that prevents its use of the reuse of the specific Pocket Vault ID." *Id*. at 4.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



TFrab at 8.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

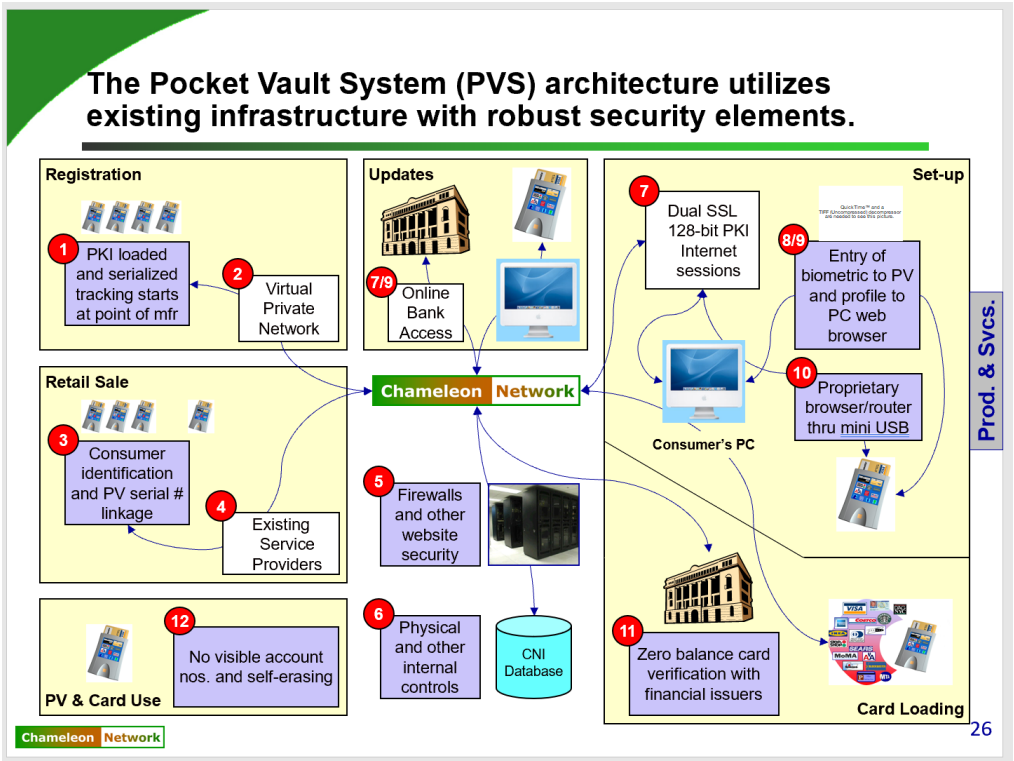
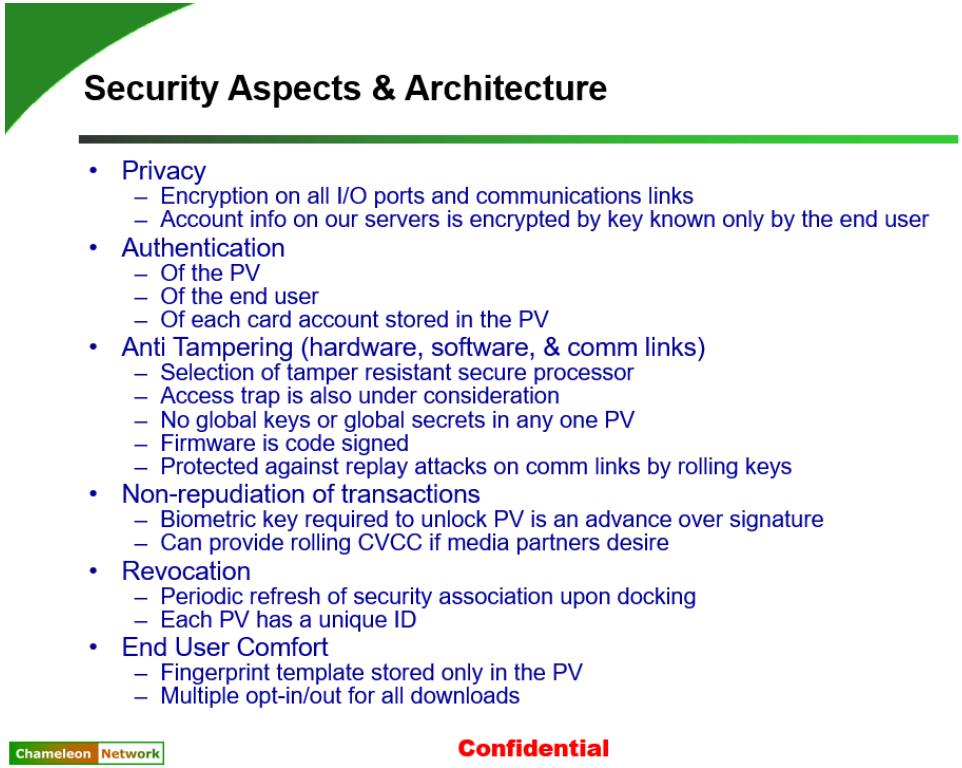
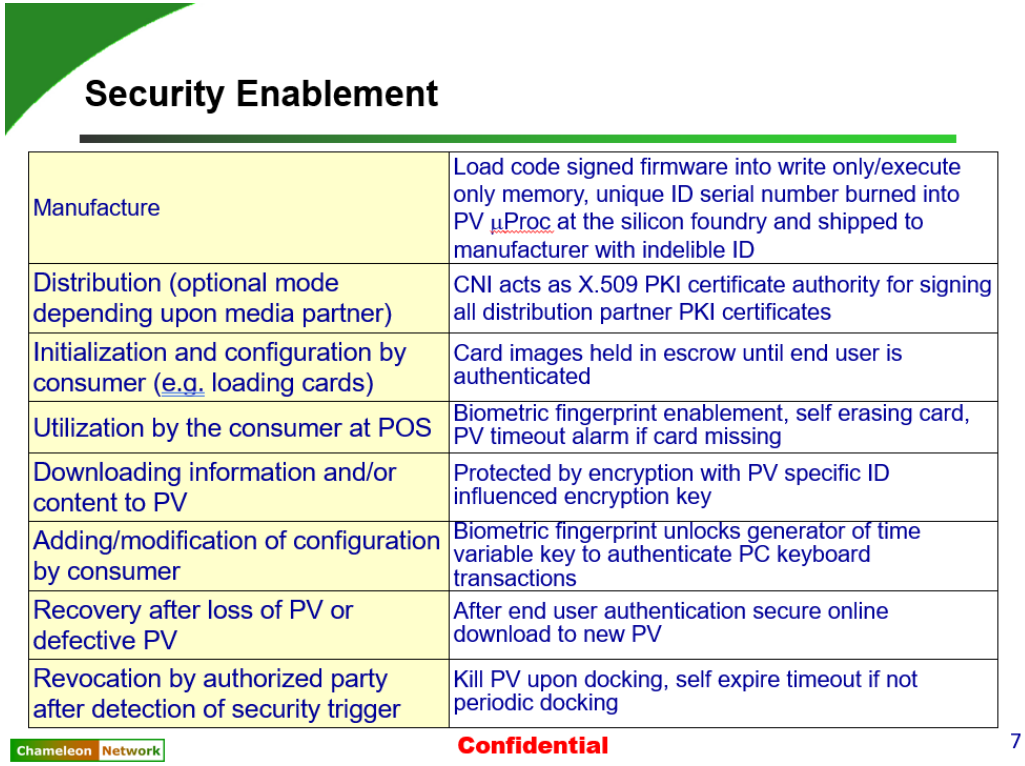
		 TFrab at 26.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



Sec3 at 6.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



Security Enablement

Manufacture	Load code signed firmware into write only/execute only memory, unique ID serial number burned into PV μProc at the silicon foundry and shipped to manufacturer with indelible ID
Distribution (optional mode depending upon media partner)	CNI acts as X.509 PKI certificate authority for signing all distribution partner PKI certificates
Initialization and configuration by consumer (e.g. loading cards)	Card images held in escrow until end user is authenticated
Utilization by the consumer at POS	Biometric fingerprint enablement, self erasing card, PV timeout alarm if card missing
Downloading information and/or content to PV	Protected by encryption with PV specific ID influenced encryption key
Adding/modification of configuration by consumer	Biometric fingerprint unlocks generator of time variable key to authenticate PC keyboard transactions
Recovery after loss of PV or defective PV	After end user authentication secure online download to new PV
Revocation by authorized party after detection of security trigger	Kill PV upon docking, self expire timeout if not periodic docking

Chameleon Network

Confidential

7

Sec3 at 7.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

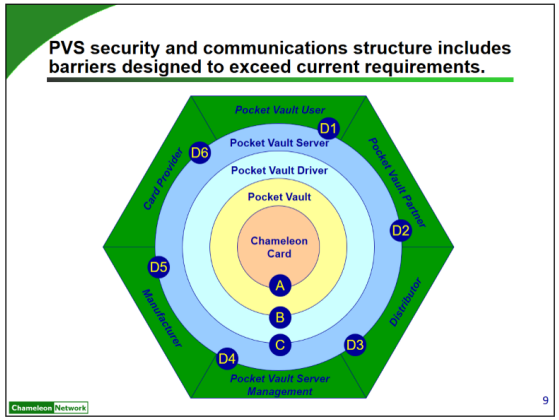
		 Barrier Technologies A Encryption, bi-directional authentication, EMV standards B https/SSL, PKI, authentication, physical connection C https/SSL, authentication, firewall, PKI D* Authentication, https/SSL, firewall D1 Requires PV session (B+C) D2 VPN, PKI D3 Post only commands D4 VPN, PKI D5 VPN, PKI D6 VPN, PKI Component Technologies CN Card Card registration, auto-erase PV commands Tamper-resistant components, fingerprint, fixed set of allowable PV Driver Trusted USB driver/router PVS Isolated subnet for database, fixed set of allowable commands Visa Intl at 9.
1I	wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a	Pocket Vault discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

	keyless lock, an ATM machine, a web site, a file and a financial account.	*See* 1H. For example, Pocket Vault discloses use of the system to create hotel room key cards to access hotel rooms. *See, e.g.*, When, at the step 2302, it is determined that the to-be-loaded file does relate to a secure media issuer, the routine 1918 proceeds to a step 2306, wherein it is determined whether the secure media issuer is a Pocket Vault participant (i.e., a media issuer having access to the network server 114). *Burger* at [0498]. "After the step 3416, the routine 3314 proceeds to a step 3418, wherein a message is displayed that indicates the card has been successfully loaded onto the Pocket Vault 102 for use in future transactions." *Burger* at [0624]. "One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time-sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who intake room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104 b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room." *Burger* at [0676]. "As shown, the routine 1400 begins at a step 1402, wherein a menu is displayed on the display 324 of the interface station computer 304 that gives the operator of the interface station computer 304 several options to choose from. These options may, for example, include: (1) the option to request that a Pocket Vault 102 be validated (i.e., permitted to store a new finger print), (2) the option to request that the information currently stored on a Pocket Vault 102 be updated (e.g., information may be uploaded from the network server 114), (3) the option to request that a transaction involving a Pocket Vault 102 be authorized, and/or (4) the option to access a website on the network server 114 and take advantage of the functionality thereof." *Burger* at [0365] Pocket Vault Overview *Pocket Vault System* replaces a consumer's conventional wallet and stores an entire wallet's contents in digital form (credit, ATM, identification, physical and network access, membership, discount cards), in a stand-alone device or integrated into PDAs and mobile phones. The Pocket Vault programs a single, "morphing" Chameleon Card to emulate the characteristics of any magnetic stripe, barcode or smart card that the user selects. The Pocket Vault and Chameleon Card are useable everywhere (brick & mortar and online), and are completely compatible with all existing point-of-sale terminals. Pocket Vault Overview.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket. "The POCKET VAULT and the Pocket Vault System are actively involved in the entire provisioning process. Because of the potential for fraud, the Pocket Vault System maintains a serialized inventory of all POCKET VAULTS. The information critical to these processes are: • The POCKET VAULT ID; • The private key for the POCKET VAULT; • The public key for the POCKET VAULT; • The private key for the Pocket Vault System; and

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		• The public key for the Pocket Vault System. The POCKET VAULT ID is a globally unique identifier (GUID) which is used as both the externally visible (i.e., used by humans) serial number and the internal identifier of the POCKET VAULT. The public and private keys are generated using standard conforming techniques. The private key (of the POCKET VAULT) only exists within a secure, tamper resistant component of the POCKET VAULT. The corresponding public key and POCKET VAULT ID are safe-stored in the Pocket Vault System. To prevent fraud, the POCKET VAULT is authenticated using the public/private key pair before any interaction with the Pocket Vault System. In addition, the Pocket vault authenticates the Pocket Vault System using the public/private key pair of the Pocket Vault System." Service Definition at 35. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." *Id*. at 22. "The RFID chip is mostly self-contained device that responds to an external wireless stimulus with a unique serial number. The RFID used in the wallet has the added ability to be turned on and off in order to allow the firmware in the wallet to decide when it is permissible for the RFID tag to respond." Spec Tob at 5. "To do this, the wallet must do at least the following: □ Store all credit card and fingerprint information in an encrypted form. □ Use a unique or random encryption method that makes each wallet different from others.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		□ Use SSL or equivalent protocol when communicating with the Chameleon Network server on the Internet. □ Not allow a debugger to connect to the processor's JTAG port and read memory contents or otherwise view any sensitive information in the clear. □ Not allow someone to load code into Flash or SDRAM, run it, and then extract sensitive information using this bogus code." *Id.* at 10-11. "Customer use e. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards.

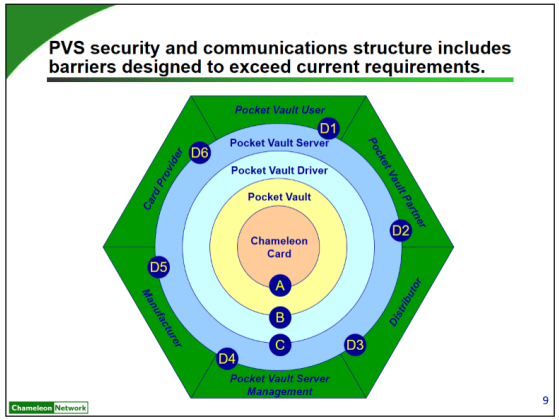
Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		4. Next the consumer can add other cards by selecting card type, category and an icon for each card. f. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor. ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

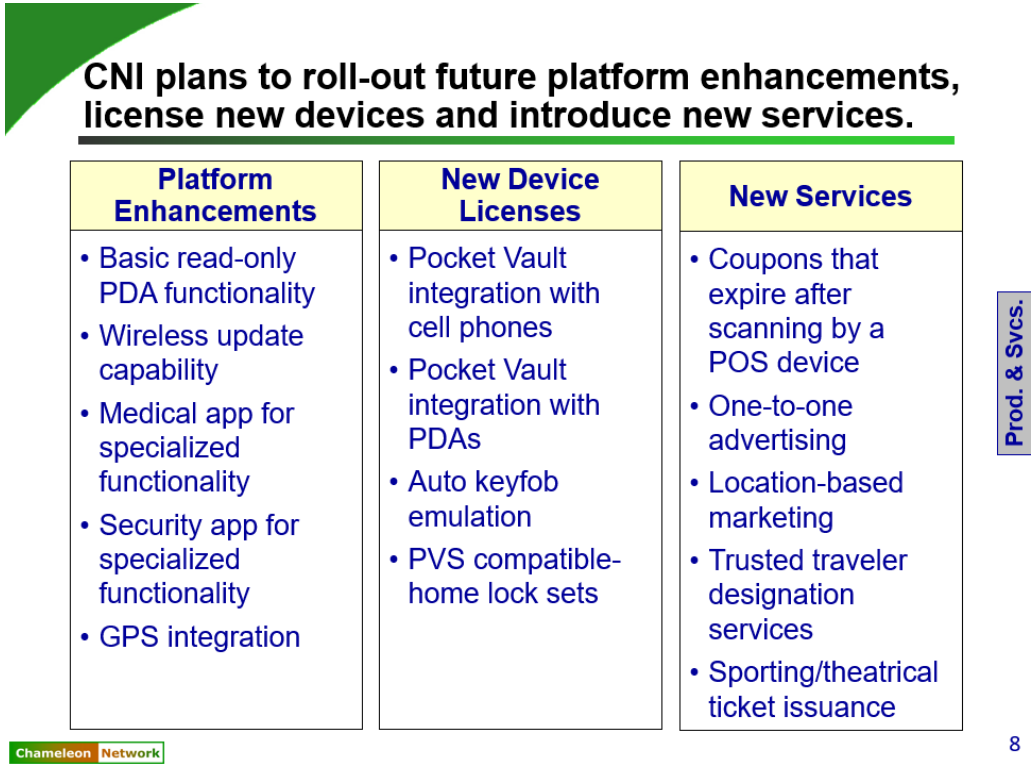
Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



Barrier	Technologies
A	Encryption, bi-directional authentication, EMV standards
B	https/SSL, PKI, authentication, physical connection
C	https/SSL, authentication, firewall, PKI
D*	Authentication, https/SSL, firewall
D1	Requires PV session (B+C)
D2	VPN, PKI
D3	Post only commands
D4	VPN, PKI
D5	VPN, PKI
D6	VPN, PKI
Component	**Technologies**
CN Card	Card registration, auto-erase
PV commands	Tamper-resistant components, fingerprint, fixed set of allowable
PV Driver	Trusted USB driver/router
PVS	Isolated subnet for database, fixed set of allowable commands

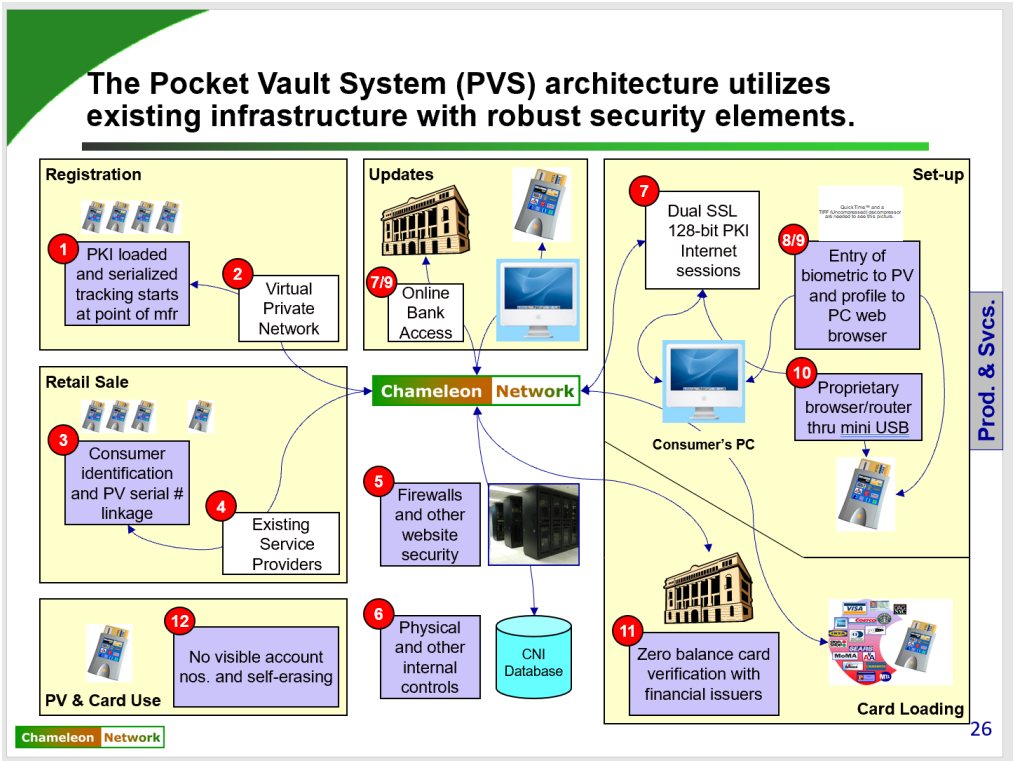
Visa Intl at 9.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



TFrab at 8.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



TFrab at 26.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

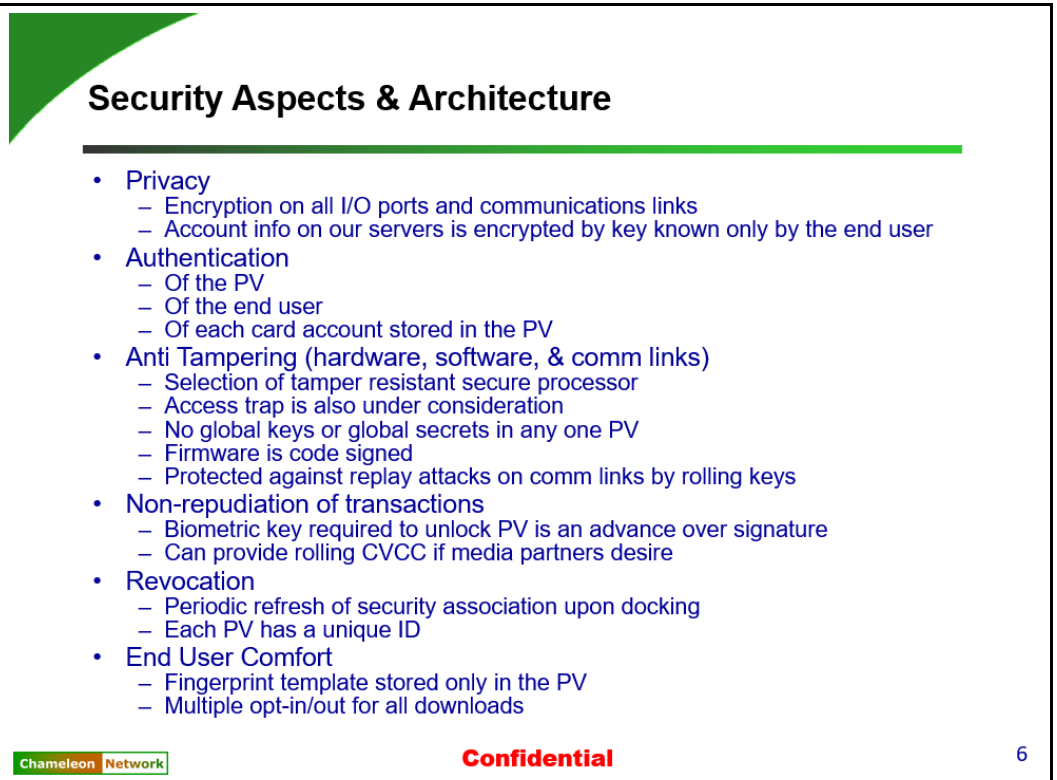
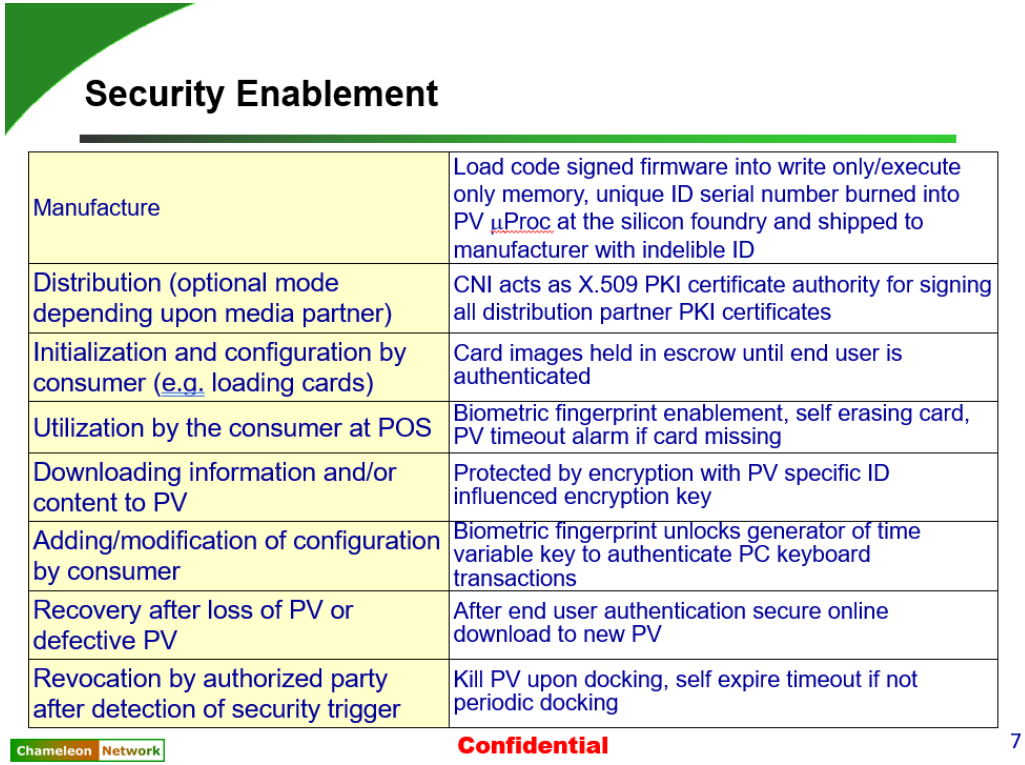
		 Sec3 at 6.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

<table>
<tr>
<td></td>
<td></td>
<td>


Sec3 at 7.
</td>
</tr>
<tr>
<td>2A</td>
<td>The method of claim 1, further comprising: Receiving a request for biometric verification, and</td>
<td>Pocket Vault discloses receiving a request for biometric verification.

See 1C.</td>
</tr>
<tr>
<td>2B</td>
<td>responsive to a determination that the scan data does not match the biometric data,</td>
<td>Pocket Vault discloses responsive to a determination that the scan data does not match the biometric data.

See, e.g.,</td>
</tr>
</table>

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"When, at the step 811, it is determined that the fingerprint scanned at the step 706 does not match any of the stored fingerprints, the routine 710 proceeds to a step 818, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215) is generated to inform the holder that the validation attempt was unsuccessful." *Burger* at [0211]. "When, at the step 1310, it is determined that the scanned fingerprint does not match any fingerprint stored in the memory 314 of the pocket vault interface unit 302, the routine 1300 proceeds to a step 1314, wherein a message is transmitted to the interface station computer 304 indicating there has been an unsuccessful attempt to authenticate an operator of the pocket vault interface unit 302." *Burger* at [0351].
2C	indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.	Pocket Vault discloses indicating the device cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code. *See* 2B
3	The method of claim 1, wherein completing the transaction includes accessing an application.	Pocket Vault discloses transaction includes accessing an application. *See* 1H.
4A	The method of claim 1, wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code	Pocket Vault discloses wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. *See* 1G-1H.
4B	includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.	Pocket Vault discloses includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party. *See* 1H.
5pre	A smartphone comprising:	Pocket Vault discloses a device.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		See 1A.
5A	a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data	Pocket Vault discloses a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data. *See* 1A.
5B	wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user	Pocket Vault discloses wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user. *See* 1B.
5C	the ID code uniquely identifying the smartphone among a plurality of smartphones	Pocket Vault discloses the ID code uniquely identifying the device among a plurality of devices. *See* 1A.
5D	the persistent storage storing the biometric data and the ID code,	Pocket Vault discloses the persistent storage storing the biometric data and the ID code. *See* 1A.
5E	the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;	Pocket Vault discloses the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the device. *See* 1A.
5F	a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,	Pocket Vault discloses a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage. *See* 1D.
5G	the validation module having a scan pad to capture scan data from a biometric scan,	Pocket Vault discloses the validation module having a scan pad to capture scan data from a biometric scan.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		See, e.g., "In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in FIG. 2." *Burger* at [0107].

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		By Michael Castelluccio, TECHNOLOGY EDITOR It doesn't have a clinical name, so let's just call it *plastigrandizing*. The symptoms in males include wallets so stuffed there are mysterious episodes of sciatic pain. In females, there are carpal tunnel-like twinges caused by repeated efforts to jam a wallet, grown to the size of a baguette, into a small purse. The cause in both cases is an ever-increasing stack of plastic cards. One obvious solution would be to reduce the number of cards you have to carry to negotiate your day. The ideal would be one card for everything-credit, debit, one pass, library, grocery-store courtesy card, video store, smart-card ID-everything. And that's what the Chameleon Network company of Concord, Mass., is working on. The Chameleon Card is aptly named, but the real genius is in the Vault (the holder) where you store the card. The Chameleon is able to replace magnetic-stripe, bar-code, and smart-card type cards because it's reprogrammable. If you want to pay with your Visa at the store, you take out the vault, press the thumbprint identifier, touch the Visa logo on the face of the card, and the card is ejected out the top with the necessary Visa information and a readout on its face announcing that it's now a Visa. The clerk swipes it, and, in 10 to 15 minutes, the card goes back to its anonymous status in its holder.  Out of Pocket.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		First-time users of the Pocket Vault will read their old credit cards with the device, which stores their information internally and backs it up to an online or local database in case the Pocket Vault is lost or stolen. Each credit card stored on the Pocket Vault is then represented by an icon on the device's touch-screen display. The Pocket Vault also prompts its owners to place their fingerprints on the device's reader pad to create a biometric profile. To use the Chameleon Card for a credit card transaction, a shopper taps the logo on the Pocket Vault's display representing the credit card account he wants to use. Seconds later, the Pocket Vault spits out the shopper's Chameleon Card, with the selected credit card account number, expiration date and logo imprinted on its flexible display, and its transducer reconfigured to work in the store's or bank's magnetic card reader. Changes Stripes. "The biometric information is stored in a secure, tamper-resistant component of the POCKET VAULT and is not stored in the Pocket Vault System." *Service Definition* at 5.4.2.1. Initialize Pocket Vault. "When the consumer gets a Pocket Vault she is instructed to go to a website. The website takes her through the instructions to: o Dock the PV set up a PV account; o Define information necessary to reliably identify the customer; o Enroll at least two fingerprints to the device; o Subsequently load cards. Note: 1) the fingerprint data never leave the device and 2) the website used for account setup can be branded by the sponsor of the PV." CitiCNI at 1. "The wallet needs to have built-in security that keeps someone from doing the following: • Gaining access to any credit card information when a valid fingerprint hasn't been read. • Gaining access to any fingerprint templates at any time." Spec Tob at §11.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"Enrollment of fingerprint and other data onto the transponder is controlled via a secure infrared link from a PC. Once fingerprints have been enrolled, the resulting templates are kept in secure memory and cannot be read out of the device. Likewise, when a fingerprint is placed on the sensor for comparison against these templates, the templates are never brought out of any silicon in an unencrypted form and hence cannot be ascertained in the clear (unencrypted) at any time during the comparison process. Fingerprint data and authorization codes are stored encrypted and the mechanical design of the device will be highly tamper resistant. The algorithms accomplishing these functions are patent pending, with a use license being afforded the Government for prototype PICS units." Märzen at 3.
5H	the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and	Pocket Vault discloses the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data. *See* 1D.
5I	a wireless transceiver that,	Pocket Vault discloses a wireless transceiver. *See* 1G.
5J	responsive to a determination that the scan data matches the biometric data,	Pocket Vault discloses responsive to a determination that the scan data matches the biometric data. *See* 1F.
5K	sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,	Pocket Vault discloses sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority. *See* 1G.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

5L	a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,	Pocket Vault discloses a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code. *See* 1H.
5M	wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.	Pocket Vault discloses wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account. *See* 1I.
6	The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network.	Pocket Vault discloses wherein the ID code is transmitted to the third-party trusted authority over a network. For example, Pocket Vault discloses communications with a network server. *See, e.g.*, "A network system 100 configured according to one illustrative embodiment of the invention is shown in FIG. 1. As shown, the network system 100 may include a portable electronic authorization device 102 (alternatively referred to herein as a "Pocket Vault") and an associated token 102 a (alternatively referred to herein as a "Chameleon Card"). Each person desiring to use the network system 100 may possess his or her own the Pocket Vault 102 and associated token 102 a. Some individuals may choose to own multiple Pocket Vaults or Chameleon Cards. The system and software therefore may accommodate the use of multiple Pocket Vaults and multiple Chameleon Cards by one individual." *Burger* at [0096]. "When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		fingerprint match, is transmitted to the interface station computer 304." *Burger* at [0349]. "According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus." *Burger* at [0019]. "When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device." *Burger* at [0186]. "When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation." *Burger* at [0524]. "All sensitive information will be encrypted during transmission over the Internet. This will be accomplished via a secure session using protocols such as HTTPS and SSL. There will be a physical separation of the Pocket Vault System web server from the Pocket Vault System database server with appropriate communications security (e.g., a firewall) between the two servers." Service Definition at 22.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		"Customer use g. Set up i. Inside the Pocket Vault box is a simple instruction form that outlines the following: 1. Plug the Pocket Vault into your PC or Mac, authenticate and the Pocket Vault will automatically seek out the Internet connection 2. From a browser on your computer, go to www."pvsponsor".com. Choose "Set up new Pocket Vault". 3. Create a Pocket Vault account. This account will be used to validate the card accounts you add to your Pocket Vault. 4. Set up your fingerprint security by following instructions on the Pocket Vault. (you will be prompted to swipe one finger from each hand three times each). 5. Verify your account by calling Chameleon Network's 800 number from your home phone (This is only done at initial setup). ii. Add cards to Pocket Vault 1. Consumer will be asked to sort the cards they want to put into the Pocket Vault into piles, one pile for the magnetic stripe cards, one for bar code cards, one for other cards. 2. The consumer will be asked to dip the magnetic cards in the Pocket Vault, which will read the card information, encrypt it, and send it to Chameleon Network's Pocket Vault System servers. a. Financial cards and certain other secure ID cards will be validated to make sure the card is active and belongs to that particular

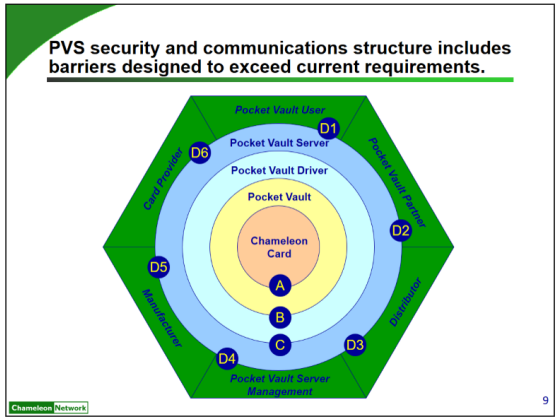
Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		consumer, and then the card information is transferred back to the device, decrypted and loaded onto the device. If the customer wants account balance information automatically uploaded to their Pocket Vault at every update, they would provide the following information at the loading of their financial cards: i. Online banking/credit card account User ID ii. Online banking/credit card Password iii. Name of bank institution (from pull down list) (This process is essentially identical to Quicken) b. Non-financial cards are loaded remotely without the validation process c. For each card added, a category (credit card, grocery ID card, discount card) determination is made by the server and this information will be confirmed with the consumer via the website 3. Next the consumer can add bar code cards through the web interface by providing pertinent information about the card (whose card it is, card number, etc.) and selecting a bar code pattern that is similar to that on the card. 4. Next the consumer can add other cards by selecting card type, category and an icon for each card. h. Financial transactions – When using the Pocket Vault for financial transactions the consumer: i. Will turn on the Pocket Vault by swiping their finger over the fingerprint sensor.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault

		ii. Selects the card they want to use (ex. Bank of America Visa, or ATM card, Mobil SpeedPass) iii. Hit the Eject icon, which transfers the card characteristics to the Chameleon Card and ejects the card. iv. Card is then swiped in the POS reader or used in the ATM machine. In the case of Mobil Speedpass the Pocket Vault is waved near the reader. v. Card is returned to the device. In Version 1, the card details are erased upon re-entry. In Version 2, the card details can also self erase if the card is left out of the PV for a specified period." Brookstone at 3-4.

Exhibit 989-L
Invalidity Chart for U.S. Patent No. 10,689,989 In View of Pocket Vault



Barrier	Technologies
A	Encryption, bi-directional authentication, EMV standards
B	https/SSL, PKI, authentication, physical connection
C	https/SSL, authentication, firewall, PKI
D*	Authentication, https/SSL, firewall
D1	Requires PV session (B+C)
D2	VPN, PKI
D3	Post only commands
D4	VPN, PKI
D5	VPN, PKI
D6	VPN, PKI
Component	**Technologies**
CN Card	Card registration, auto-erase
PV commands	Tamper-resistant components, fingerprint, fixed set of allowable
PV Driver	Trusted USB driver/router
PVS	Isolated subnet for database, fixed set of allowable commands

Visa Intl at 9.